Techniques in Secure Chaos Communication

A PhD Thesis by Yuu-Seng Lau

(B. Eng. Elect. Eng., B.Sc. Comp. Sci.)

School of Electrical and Computer Engineering

Science, Engineering and Technology Portfolio

RMIT University

Melbourne, Victoria, Australia

February 2006

Declaration

I certify that except where due acknowledgement has been made, the work is that of the author alone; the work has not been submitted previously, in whole or in part, to qualify for any other academic award; the content of the thesis is the result of work which has been carried out since the official commencement date of the approved research program; and, any editorial work, paid or unpaid, carried out by a third party is acknowledged.

Signed: ..... Date: .....

Yuu-Seng Lau

Acknowledgements

I would like at this juncture to express my deepest appreciation and gratitude to my kind supervisor Associate Professor Zahir M. Hussain for his support, unlimited assistance and beneficial advice throughout my candidature at RMIT University. It has been a great pleasure and privilege to work with him and to benefit from his rich knowledge and experience. His door is open to me whenever I seek help. Thanks and deepest appreciations are extended to Professor Richard Harris, ex-director of the Centre for Advanced Technologies in Telecommunications (CATT), RMIT University, for his support and guidance, especially during my first days at RMIT. Dr. Zahir Hussain, myself and other PhD students have had a wonderful and fruitful collaboration. They gave their time and effort so generously, and showed me the true spirit of academic supervision and collaboration.

I gratefully acknowledge the support of other RMIT PhD students and RMIT staff who were in the CATT and at the School of Electrical and Computer Engineering (SECE): Dr. Kevin Lin, Lei Shang, Jusak Jusak, Dr. Seedahmed Mahmoud, Dr. Adam Thompson, Suyong Eum, Robert Suryasaputra, Suresh Venkatachalaiah, Tasso Athanasiadis, Katrina Neville, Dr. Irena Atov, Dr. Alexander Kist, Dr. Horace King, Andrew Cassin, and other staff whom have provided a great deal of support in discussions to relate my work to their exper-

tise fields. My thanks also extended to RMIT University for financial support in waiving the School fees during my PhD candidature 2002-2005.

Thanks and appreciation to all of my close friends Min Chen, Adeline, Leeping, Jasmine, Hui Ling, Hui Meen, Meen Meen, Shelly, Aichin, Graeme Class, Tom Kiing, Happy, Alfred, Joyce, Zufendy, and Lik Hing, who cared for me when I am sick, hungry and emotionally supported me during my ups and downs while doing my PhD. A special thank to my very special one Augustina Lo aka Lushelly whom has give me mentally and emotionally support during my PhD thesis write up, without her my thesis would not have completed.

Last but not least, I would like to thank all my relatives and family members for their long-term support, encouragement, care and love for me since I was young until now. Their love and care is the driving power for my study and my life.

Contents

List of Figures

List of Tables

Acronyms

2G	Second generation
3G	Third-generation
3GPP	Third-generation partnership project
4G	Fourth-generation
AoA	Angle-of-arrival
AWGN	Additive white Gaussian noise
BER	Bit error rate
BPSK	Binary phase shift keying
BS	Base station
CDMA	Code division multiple access
CMA	Constant modulus algorithms
COOK	Chaos on off key
CSK	Chaos shift keying
CSK-OFDM	Chaos shift keying-Orthogonal frequency division multiplexing
CSK-WOFDM	Chaos shift keying-wavelet based
	Orthogonal frequency division multiplexing
DAB	Digital audio broadcasting
DCSK	Differential chaos shift keying
DFT	Discrete Fourier transformation
DS-CDMA	Direct-sequence code division multiple access

DSL	Digital subscriber line
DVB	Digital video broadcasting
DWT	Discrete wavelet transformation
EVD	Eigen-value decomposition
FDMA	Frequency division multiple access
FFT	Fast Fourier transformation
FIR	Finite impulse response
FM	Frequency modulation
FWV-LMS	Fixed forward prediction weight vector least mean square
GBHDS	Geometrical-based hyperbolic distributed scatterers
GSM	Global system for mobile communications
IDFT	Inverse discrete Fourier transformation
IDWT	Inverse discrete wavelet transformation
IFFT	Inverse fast Fourier transformation
ISI	Inter-symbol-interference
LCG	Logistic chaos generator
LFM	Linear frequency modulation
LMS	Least mean squared
LOS	Line-of-sight
MAI	Multiple access interference
MCM	Multi-carrier modulation
MC-CDMA	Multi-carrier division multiple access
MIMO	Multiple-input multiple-output
MLD	Maximum likelihood detector
MMSE	Minimum mean-square error
MS	Mobile station
MSE	Mean-square error

NG	Next generation
OFDM	Orthogonal frequency division multiplexing
O-STBC	Orthogonal space-time block coding
PAPR	Peak-to-average power ratio
pdf	Probability density function
PLC	Power line communication
PN	Pseudo noise
psd	Power spectral density
PSK	Phase shift keying
QAM	Quadrature amplitude modulation
QFM	Quadratic frequency modulation
QPSK	Quadrature phase shift keying
RLS	Recursive Least Squares
SER	Symbol error rate
SF	Spreading factor
SIR	Signal-to-interference ratio
SNR	Signal-to-noise ratio
STBC	Space-time block coding
SS	Spread specturm
TDD	Time division duplexing
TDMA	Time division multiple access
TV-LMS	Time varying least mean square
ULA	Uniform linear array
UWV-LMS	Updated forward prediction weight vector least mean square
WCDMA	Wideband CDMA
WOFDM	wavelet based Orthogonal frequency division multiplexing
WV-LMS	weight vector least mean square

Chapter 1

Introduction

Chaos theory, a branch of the theory of the interesting nonlinear systems, exhibits an interesting nonlinear phenomenon and has been intensively studied in the past four decades. Initially, it was studied by researchers with strong mathematical background rather than circuit-designers or electronic engineers/ scientists. This is mainly due to the fact that circuit design and implementation cannot match up with the mathematical equations needed due to technical and practical problems. With the advance in circuit technology and digital signal processing in the past few decades, the use of chaos phenomena in daily real-life engineering products become possible. Various applications and products were reported, including but not limited to the following; utilizing the advantage of chaotic dynamic behaviour in washing machine technologies, reaction rate control in chemical technologies, treating cardiac arrhythmia and providing a secure communication channel by using a chaotic carrier. Therefore, more and more applications have utilized chaos theory. We are particularly interested in the area of secure communications.

Chaotic signals in the time domain are neither periodic nor quasi-periodic and are unpredictable on the long term. This unpredictable phenomenon man-

ifests itself as a wideband noise-like power spectrum in the frequency domain. The chaotic dynamic system can be classified into continuous-time and discrete-time. A set of differential equations can be used to derive a continuous-time chaotic system as shown below:

$$g(x,t) = \dot{x}, \quad x(t_0) = x_0 \tag{1.1}$$

where g is the set of differential equations to define the dynamical system, x is a vector represents the current state of the system at time t. In our thesis, we will focus on discrete time chaotic systems, the chaotic signal sampled at k^{th} iteration can be given by:

$$x_k = g(x_{k-1}) = g^{(k)}(x_0) \tag{1.2}$$

where x is the state vector, and $g(\cdot)$ is the iterative function also known as "chaotic map".

In addition to it random and non-periodic behaviours, another unique property of chaotic systems is their bifurcation behaviours, where the chaotic system is sensitive for environment changes and highly dependent on its initial conditions. Small difference in the initial condition produces a very different chaotic signal after a short time period. This phenomenon is illustrated and shown in Chapter 3. Therefore, one can produce a large number of chaotic signals even with a very simple dynamic deterministic equation. The auto- and cross-correlation properties of a chaotic signal are also shown in Chapter 3 to have a white noise like behaviours. The impulse like nature of these correlation functions explain why the power spectrum of the chaotic signal exhibits a wideband feature. These wideband and noise like features of a chaotic signal are particu-

larly good in spread-spectrum communications.

In conventional spread-spectrum communications, the narrowband signal modulated into a wideband carrier increases the signal bandwidth substantially and can be transmitted in a low power spectral density (psd) environment without affecting the bit error performance. As such, the transmitted signal is hidden under the background noise to provide a secure communication channel with a low probability of detection from unintended parties. In addition, with carefully designed and selected spread sequence which benefits from a good correlation property can accommodate multiple access technologies, meaning multi-user transmission in parallel. The wideband signals can also provide an anti-jamming capability when special demodulation technique is applied. Another advantage of using wideband signals in wireless communication is their ability to combat wireless propagation noise effects such as multipath and intersymbol interference (ISI). Multipath occurs when the transmitted signal propagates through different paths and directions from the transmitted path which leads to multiple copies of transmitted signal with different delays to be received. These multiple copies and reflected waves interfere with each other causing ISI. Under wideband transmission, we can easily differentiate these paths with a RAKE receiver or combat it with an advanced signal processing technique such as adaptive equalization. Such problems are widely studied in the past and has been applied in our real world second (2G) and third generation (3G) mobile communication.

A chaotic signal having a wideband nature benefits itself in spread-spectrum communications. The use of chaos-based system offered several advantages over the conventional methods. Firstly, chaotic signals are much easier and faster to generate using a simple circuit. Hence, reduction in hardware cost is obtained. Secondly, the non-periodic and bifurcation behaviours of the chaotic signal can-

not easily be intercepted and predicted, thus, an increase in system security is obtained. In addition, a large number of chaotic signals can be generated which is useful in multi-user environment. All kinds of schemes utilizing chaos properties have been proposed in last decade and showed to provide advantage in terms of security, capacity, and BER performance.

In many real world problems such as those associated with chaos signals, one only has little information about what the state variables of the dynamical system and has no hope of observing them. Instead, we can utilize the adaptivity of an adaptive algorithm to try to estimate and track this unknown state variables. Adaptive algorithms have been widely studied in the past and used in too many applications. In the communication arena, they have been applied for noise reduction, demodulation, multi-user detection, channel estimation, channel equalization, system identification, signal synchronization, etc. Recently, adaptive algorithms have been applied in chaos communications (as show in chapter 6 and chapter 7).

Chaos-based communication systems have been shown to provide certain advantages over conventional communication systems. However, there are still plentiful of issues to be resolved before chaos-based systems can be put into practical use. Hence, a study on the use of adaptive algorithms to improve chaos communication makes it possible for further practical improvement. More research is needed in this area and there is a plenty of room for further study and improvement.

1.1 Objectives of This Dissertation

This dissertation is concerned primarily with secure chaos communication and adaptive algorithms for secure chaos communication. The study has focused on the physical link secure communication signal utilizing chaos bifurcation behaviours and adaptivity is also handled. The thesis also deals, to a lesser extent, with areas of general interest in wireless communication and applied signal processing. The main accomplishments documented in the thesis are:

1. To evaluate the use of chaos theory in different communication schemes.
2. To establish a framework for wireless multimedia secure communications.
3. To develop a logistic map that enhances security and performance. A secure CSK communication model is proposed.
4. To extend the space-time diversity signal enhancement technique in wireless chaos communications.
5. To evaluate the use of different adaptive algorithms in chaos communication.
6. To apply blind adaptive multiuser detection technique for chaos CDMA communication. Performance comparison with conventional CDMA communication is tackled.
7. To develop a new kind of adaptive beamforming utilizing the filter weight factor for chaos communication signals and general communication signals.
8. To develop, extend, and evaluate the adaptive noise reduction technique in chaotic signal environment for the use in chaos communication.

1.2 Contributions of This Dissertation

This dissertation has contributed to two major study areas: chaos communications and adaptive chaos applications. The main contributions of this dissertation are as follows

1. A Time-dependent Adaptive LMS algorithm for noise reduction have been proposed. It is shown that the new algorithm outperforms the conventional schemes in terms of convergence speed and minimum mean-square error. This work was published in *Australian Telecommunications Networks and Applications Conference 2003* [1, 2] and in *WSEAS Transactions on Circuits and Systems* 2004 [3].
2. A Weight vector LMS algorithm for adaptive beamforming has been proposed. Both fixed forward prediction weight vector LMS (FWV-LMS) and updated forward prediction weight vector LMS (UWV-LMS) algorithms shown to provide better tracking ability and shown to provide better minimum mean-square error than the conventional method. This model was presented at *IEEE Region 10 International Conference on Analog and Digital Techniques in Eletrical Engineering 2004* (*TENCON'04*), Thailand [4].
3. A review for adaptive blind multiuser detection technique and correlator receiver is provided. A comparative study for Chaos-CDMA and PN-CDMA using this techniques are presented. The work was published in *IEEE Region 10 International Conference on Analog and Digital Techniques in Eletrical Engineering 2005* (*TENCON'05*), Melbourne [5]
4. A modified logistic chaotic generator (LCG) for chaos shift-keying has been proposed. The newly proposed LCG provides an extra bifurcation

parameter that can be used to enhance security performance or as a multiple access parameter. A multimedia framework is provided in conjunction with the proposed LCG. The work is submitted to *Multimedia Cyberscape Journal* for review [6, 7].

5. A review for chaos communication and its multi-carrier modulation schemes; chaos code division multiple access (chaos CDMA), chaos shift-keying Orthogonal frequency division multiplexing (CSK-OFDM), chaos shift-keying wavelet based OFDM (CSK-WOFDM), and chaos based CDMA-OFDM is provided. In general, chaos based communication provides better bit-error rate (BER) performance. The results were published in [8, 9] and *WSEAS Transactions on Communications* [10].
6. The space-time diversity wireless signal enhancement technique is applied in chaos shift-keying communication. It is shown that both adaptive eigenbeamforming and orthogonal space-time block coding (OSTBC) diversity technique can be applied in chaos communication systems. The findings of this work were published in *IEEE Region 10 International Conference on Analog and Digital Techniques in Eletrical Engineering 2005* (*TENCON'05*), Melbourne [11].

1.2.1 Publications by the author

Below is the list of publications in conjunction with the PhD candidature of the Author:

Journal Publications

1. **Yuu-Seng Lau**, Zahir M. Hussain, and Richard Harris "A Time - Dependent LMS Algorithm for Adaptive Filtering," *WSEAS Transactions on Circuits and Systems*, Issue 1, Volume 3, January 2004.

2. **Yuu-Seng Lau** and Zahir M. Hussain, "Chaos Shift Keying Spread Spectrum with Multicarrier Modulation for Secure Digital Communication," *WSEAS Transactions on Communications*, Issue 1, Volume 4, January 2005.

Refereed Conference Publications

1. **Yuu-Seng Lau**, Zahir M. Hussain, and Richard Harris, "A Time - Varying Convergence Parameter for the LMS Algorithm in the Presence of White Gaussian Noise," in *Proc. Australian Telecommunications, Networks and Applications Conference*, (*ATNAC'03*), Melbourne, Dec. 2003.

2. **Yuu-Seng Lau**, Zahir M. Hussain, and Richard Harris, "Performance of Adaptive Filtering Algorithms: A comparative Study," in *Proc. Australian Telecommunications, Networks and Applications Conference*, (*ATNAC'03*), Melbourne, Dec. 2003.

3. **Yuu-Seng Lau**, Zahir M. Hussain, and Richard Harris "A Time - De-

pendent LMS Algorithm for Adaptive Filtering," *The WSEAS International Conference on ELECTRONICS, CONTROL and SIGNAL PROCESSING*, (*ICECS'03*), Singapore, Dec 2003.

4. **Yuu-Seng Lau**, Zahir M. Hussain, and Richard Harris, "A Weight-Vector LMS Algorithm for Adaptive Beamforming," in *Proc. IEEE Region 10 International Conference on Analog and Digital Techniques in Electrical Engineering*, (*TENCON'04*), ChiangMai, Nov. 2004, pp.

5. **Yuu-Seng Lau** and Zahir M. Hussain, "Chaos Shift Keying Spread Spectrum with Multicarrier Modulation for Secure Digital Communication," *The 4th WSEAS International Conference on Signal Processing, Computational Geometry and Artificial Vision*, (*ISCGAV'04*)Greece, Dec 2004.

6. **Yuu-Seng Lau** and Zahir M. Hussain, "Chaotic-Based CDMA Versus PN-Based CDMA for Digital Secure Communications: A Comparative Study," in *Proc. Australian Telecommunications, Networks and Applications Conference*, (*ATNAC'04*), Sydney, Dec. 2004

7. **Yuu-Seng Lau** and Zahir M. Hussain, "Chaotic-Based OFDM-CDMA for Secure Digital Communications: Performance Comparison with PN-based OFDM-CDMA," in *Proc. 3rd Workshop on the Internet, Telecommunications and Signal Processing*, (*WITSP'2004*), Adelaide, Dec. 2004.

8. **Yuu-Seng Lau** and Zahir M. Hussain, "A New Approach in Chaos

Shift Keying for Secure Communication," in *Proc. IEEE International Conference on Information Technology and Applications*, (*ICITA'05*), Sydney, July 2005.

9. **Yuu-Seng Lau**, Kevin. H. Lin, and Zahir M. Hussain, "Space-Time Encoded Secure Chaos Communications with Transmit Beamforming," in *Proc. IEEE TENCON*, (*TENCON'05*), Melbourne, Nov 2005.

10. **Yuu-Seng Lau**, Jusak Jusak, and Zahir M. Hussain, "Blind Adaptive Multiuser Detection for Chaos CDMA Communication," in *Proc. IEEE TENCON*, (*TENCON'05*), Melbourne, Nov 2005.

Submitted Papers

1. **Yuu-Seng Lau**, Tasso Athanasiadis, and Zahir M. Hussain, "A Secure Chaos Digital Communication for Multimedia application," *Submitted to Multimedia Cyberscape Journal*, 2005.

1.3 Organization of the Dissertation

This dissertation consists of nine chapters, organized as follows:

Chapter 2 Overview of Chaos Communications. This chapter gives a brief description of chaos theory and it history that prepares the readers to later applications in communication. A comprehensive review of chaos theory

and its applications in engineering is presented. Next, we provided a background overview of adaptive algorithms and their applications in modern wireless communication.

Chapter 3 Secure Chaos Communication and It Applications. In this chapter, we proposed a modification of a kind of LCG maps to provide an extra parameter which can be used as a security parameter or a multi-user parameter. A comprehensive study of the proposed model is carried out in conjunction with a proposed secure digital multimedia framework, with numerical simulation and performance study. Finally, the security effect and issues of this secure multimedia framework are discussed.

Chapter 4 Space-Time Diversity for Chaos Communication. The space-time diversity wireless signal enhancement technique is introduced to the secure chaos communication in this chapter. In order to enhance the security of the chaos signal, the proposed framework first encodes the chaos chip-symbols into orthogonal space-time block codewords and transmit these codewords in the eigen-directions of the wireless channel to provide diversity in the spatial domain. In this chapter, we investigate the performance improvement from such combination over a macrocell channel model that is originally proposed in [12] and proved to be a realistic model.

Chapter 5 Chaos in Multi-Carrier Communications. Chapter 5 provides an overview of chaos multi-carrier communications. A combination of different chaos communication techniques and different multi-carrier modulation techniques are presented. This led to a performance comparative study for different scheme combinations including: CSK-OFDM vs CSK-wavelet based OFDM,

Chaos-CDMA vs PN-CDMA multi-user environment, and Chaos-CDMA-OFDM vs PN-CDMA-OFDM.

Chapter 6 Blind Adaptive Multiuser Detection for Chaos CDMA Communication. In this chapter we implemented an adaptive constant modulus algorithm (CMA) for multi-user detection in Direct Sequence Code Division Multiple Access (DS-CDMA) systems to mitigate the multi-user access interference. We evaluated the performance of the multi-user detection technique utilizing the adaptive CMA scheme against the common used correlator scheme. Simulation results for both techniques are presented and shown in general that chaos-CDMA outperforms PN-CDMA for both detection schemes.

Chapter 7 Weight-Vector LMS Algorithms for Adaptive Beamforming in Chaos Communication. In this chapter we presented two new weight-vector adaptive LMS algorithms (WV-LMS) for minimum mean square error (MMSE) beamforming adaptive algorithm. The conventional adaptive LMS algorithm has been utilized in array antenna beamforming to direct the radiated power towards the desired signal and null the multipath signals. Rather than using a fixed convergence parameter μ in the conventional LMS algorithm, the two proposed algorithms exploit the useful information in the forward prediction of the weights vector. We used the forward prediction of the weights vector to dynamically change the convergence parameter μ_n. Both algorithms have been tested for beamforming and have been shown to provide better MMSE performance than the conventional LMS.

Chapter 8 Adaptive Algorithms for Performance Enhancement in Chaos Communication. In this chapter we developed a time-varying conver-

gence parameter μ_n with time-decaying law for adaptive noise reduction filtering technique. A comparative performance study for the proposed TV-LMS algorithm and other two main adaptive approaches: the least-mean square (LMS) algorithm and the recursive least-squares (RLS) algorithm are presented. The proposed technique leads to faster convergence and provides reduced mean-squared error as compared to the conventional fixed parameter LMS algorithm.

Chapter 9 Conclusion and Future Directions. Although each chapter in this dissertation presents its own concluding remarks, we summarized the main conclusions of this dissertation and possible future directions in Chapter 9.

Chapter 2

Overview of Chaos Communications

2.1 Chaos Theory in Communications

2.1.1 Introduction

Living in today's fast paced world facing advancing technologies, we are exploring every possible way to enhance our life style. In order to achieve this goal, scientists usually have to return to the very basics and study the nature of our world. However, due to the dynamic, non-linear and unpredictable properties the real world exhibits, it is difficult to model it using a simple mathematical formula. In most textbooks, linear deterministic mathematical models applied to these dynamics revealed three types of behavior: convergence towards periodic solution, convergence towards a quasi-periodic solution, or a solution that approaches a constant.

Only part of the real world myth can be solved with these types of systems, thus requires a more effective and accurate solution. A solution that reflects the unpredictable nature of our world is the "Chaos Theory". It provides the required kind of system behavior (non-linear, dynamic, unpredictable

and etc), thus it has been widely studied by mathematicians and scientists alike. A chaotic system is a deterministic system that exhibits non-linear systems behavior with certain distinguished features [13, 14, 15, 16]. There are a lot of definitions for the chaotic system, which is in simple term "A system that becomes aperiodic (non-linear) if its parameter, internal variable, external signals, control variable, or even initial value is chosen in a specific way", we call this unpredictable behavior of a deterministic system as chaos theory or chaos system.

2.1.2 Chaotic Map

Chaos theories have been widely studied in the past; a vast number of different forms of mathematical models are derived and investigated. Generations of chaotic maps came from many different directions. It can be a complex or simple control system, a mathematical equation such as a differential equation, or a simple circuit modelling like Chua circuit.

One of the very early chaos theories started in early 1900's as studied by Henri Poincare on the problem of motion of three objects in a mutual gravity attraction. By solving this module, he has paved a way to analyse a complex system in a much easier way using a reduced system with all the key features of the original. Here, a continuous motion in the n-dimensional space projected on Poincare section can be represented using discrete transformation (map) M in the (n-1)-dimensional space on the intersection of a trajectory with the same side of surface.

$$P_{n+1} = M(P_n) \tag{2.1}$$

Henry Poincare found that there can be orbits which are nonperiodic, and yet not forever increasing nor approaching a fixed point. Since then, a lot of other classes of chaos theory had been derived from the topic of linear and nonlinear differential equation include famous Smale horseshoe map, Lyapunov exponent, Lorenz Equation, Kolmogorov Entropy, etc.

In this thesis, we will concentrate on simple polynomial mapping which exhibits chaotic behaviour that arises from simple non-linear dynamical equation. Such a mathematical model of chaos theory often involves repeated iteration of simple mathematical formulas. This type of mapping is called logistic map. Mathematically it can be written as:

Logistic Map 1

$$g_{n+1} = 1 - 2g_n^2 \tag{2.2}$$

Logistic map 1 is one of the simplest chaos logistic maps used to generate chaotic signals. This map has been used in a number of applications including digital communications [17, 18, 19]. Its properties have been widely studied. In order to converge this logistic map 1 to a chaotic logistic map, the initial condition for g_0 has to be in the interval [-1, 1].

Logistic Map 2

$$g_{n+1} = ag_n(1 - g_n) \tag{2.3}$$

Logistic map 2 is another dynamic system that is capable of exhibiting chaotic properties. This logistic equation is sometimes referred to as the Ver-

hulst model. Introduced by Pierre Verhulst in the mid 18-th century, it is used to model population growth. Mathematicians have studied this discrete quadratic recurrence equation for centuries and found that it exhibits chaos behavior when the bifurcation parameter (or control factor) a is in the interval of $3.57 < a \leq 4$; for a non-periodic chaos system. This map has also been proposed for spread spectrum communication [20, 21]

Other Chaotic Maps

In this thesis much of the study is focused on the above two logistic maps (logistic map 1 and logistic map 2). There are, nevertheless, a lot of other chaotic maps that can be applied in communication. Such chaotic generators are listed but not limited to below:

Bernoulli map

$$g_{n+1} = 2g_x \pmod 1 \tag{2.4}$$

Bernoulli map, also known as dyadic map, has been used in communication as in [22, 23].

Henon map

$$g_{n+1} = 1 - ag_n^2 + y_n \tag{2.5}$$

$$y_{n+1} = bg_n \tag{2.6}$$

Henon map is one of the simplest 2-dimensional invertible maps. The map was introduced by Michel Henon as a simplified model of the Poincare section of the Lorenz model. It has been proposed in communication by [24, 25, 26, 27]. Henon map can also be

represented in other forms as shown below:

$$g_{n+1} = g_n \cos(a) - (y_n - g_n^2) \sin(a) \tag{2.7}$$

$$y_{n+1} = g_n \sin(a) + (y_n - g_n^2) \cos(a) \tag{2.8}$$

Ikeda map

$$g_{n+1} = a + b(g_n \cos(t_n) - y_n \sin(t_n) \tag{2.9}$$

$$y_{n+1} = b(g_n \sin(t_n) - y_n \cos(t_n)) \tag{2.10}$$

$$t_n = \alpha - \frac{\beta}{1 + g_n^2 + y_n^2} \tag{2.11}$$

Ikeda map is also one of the most studied chaos map that applied in communication [28, 29, 30]. The standard parameter values for Ikeda map are $a = 1$, $b = 0.9$, $\alpha = 0.4$ and , $\beta = 6$.

Further studies of all of the above maps are needed to examine their use in different communication schemes. In Chapter 3 we proposed a modification of logistic map 2 for chaos shift-keying (CSK) communication. It is noted that, different chaos generators may be useful and beneficial to different communication schemes. Hence, a careful selection of chaos generator is needed for different communication schemes.

2.1.3 Wireless Communication

Despite all the work that has been done by all the great mathematicians on chaos theory, it is only the recent event done by Pecora and Carroll [31] on chaos synchronization that brought our attention to the use of chaos in communication. The bifurcation property of a chaos system makes the synchro-

nization seems futile in chaotic communication. However, Pecora and Carrol have proved both theoretically and experimentally that if the chaos system is divided into a master-slave configuration, the two chaotic signals can be synchronized. This discovery generated a lot of interest in exploring the potential applications of synchronized chaos in communication and provided a bridge between chaos theory and practical implementation of chaos communications. However, the synchronization process requests a more complex chaos system that can be partitioned into master-slave configuration; such a system requires a more sophisticated (generally multi-dimensional) chaos system like Lyapunov exponents, Lorenz equation, and etc.

In wireless communication, the primary objective of the synchronization process is to recover and track the basic signal from the noisy received signal and maximizes the probability of correctly identifying the transmitted symbols. Despite the fact that chaos theory in communication has claimed advantages over conventional methods, it is still a difficult problem due to the sensitivity of the demodulation process to take place in real world applications. In a coherent receiver, synchronization is commonly used as a technique to recover the sample function from the received waveform as a reference signal for a correlator. This type of receiver suffers from high sensitivity to parameter mismatche between the transmitter and the receiver. Moreover, the synchronization process also introduces a few drawbacks in terms of synchronization time, circuit complexity, and severe penalties associated with the loss of synchronization [32]. Hence, under poor propagation conditions, communication without synchronization may be preferable. On the other hand, adaptive algorithms may be useful in these noisy channel environments. In this case the sensitivity drawback in chaos communication schemes, which introduces mismatch parameters, can be exploited

to find unknown slave system parameters [33]. Indirectly, this can be used to control the slave system by means of tuning its parameters adaptively until synchronization occurs. Some examples of chaotic communication schemes with or without synchronization are given in [34]. Non-coherent receivers which use the decorrelation properties of the chaotic signals showed to be more robust to channel noise. However, this type of receivers rely on the long term decorrelation properties of the transmitted signal. This led their performance to be close to the conventional (pseudo-noise or pseudo-random) spread-spectrum communication. In both cases, both coherent and non-coherent receivers for chaos communication can dramatically improve the performance when a noise reduction or signal separation technique is employed. Again, adaptive algorithms will certainly be a useful tools for chaos communication.

In this thesis, we focus our research on the use of chaos theory in wireless communication arena, particulary in the spread spectrum digital communication. Chaos signal can be used to transmit both analog and digital signals. In modulating an analog signal, chaos parameter modulation and chaos masking are two commonly found methods in the literature [35, 36, 37, 38, 39, 40, 41]. On the other hand, chaos shift keying (CSK), differential chaos shift keying (DCSK), chaos On Off Keying (COOK), and chaos CDMA are used to modulate digital signals [42, 43, 44, 45, 46, 47, 48]. In this thesis, we are particularly interested in CSK and Chaos-CDMA. The performance of these systems can vary depending on the channel environment and also on the demodulation method. Adaptive algorithm demodulation is also studied. In the following, we provide a brief summary of some of the above mentioned schemes.

Chaotic Masking Modulation

Chaos Masking Modulation can utilize the chaos signal as a communications carrier. Chaos masking can be used to mask and transmit both analog and digital signals. The transmitted signal $s(t) = x(t) + m(t)$, where the original message $m(t)$ is added to a chaos signal $x(t)$. This work more or less like amplitude modulation (AM). The masking scheme can work only when the amplitude of the information signal is much smaller than that of the masking chaos signal. At the receiver, the masking signal is then subtracted from the received signal to retrieve the original information [49, 50]. Therefore, the performance of this scheme is largely dependent on the synchronization ability of the chaotic system.

Chaos Parameter Modulation

Chaos parameter modulation scheme is to embed the information signal into the chaos bifurcation parameter [40, 41]. For example, in LCG2, we know that the bifurcation parameter can be in the range of $3.57 < a \leq 4$. As a result, rather than using a fixed (constant) value for parameter a, we can actually inject the information into parameter a. In another word, the bifurcation parameter will vary within the range but now depends on the information signal. At the receiver, challenge lays in the design of a retrieval scheme for the bifurcation parameter variation from the received signal (which may distorted by channel noise). This scheme is highly sensitive to channel noise. Under noise-free condition, ideally to recover the information signal is only to find an inverse function of the transmitter signal. However, when noise is present, the scheme can perform very badly. Recently, an adaptive algorithm is used to enhance on

the demodulation for this scheme under noisy environment and has shown huge improvement in recovering the information signal [40, 41].

Chaos Shift Keying (CSK)

In binary chaos shift keying modulation, chaotic signals carrying different bit energies are used to transmit the binary information [7, 17, 18, 43, 51, 52]. An information signal is encoded by transmitting one chaotic signal $x_1(t)$ or $x_0(t)$ at a time. For example, if the information signal binary bit "1" occurrs at time t, the chaos signal $x_1(t)$ is to be sent, and for information bit "0", the chaos signal $x_0(t)$ is to be sent. The two chaotic signals can come from two different chaos systems or the same system with different parameters. The transmitted signal is given by

$$s(t) = \begin{cases} x_1(t) & \text{, symbol "1" is transmitted} \\ x_0(t) & \text{, symbol "0" is transmitted} \end{cases} \tag{2.12}$$

In this thesis, we concentrate on antipodal CSK modulation technique. Both of the chaotic signals are inverted copies of each other ($x_0(t) = -x_1(t)$). The transmitted signal can then be expressed as

$$s(t) = \begin{cases} x_0(t) & \text{, symbol "1" is transmitted} \\ -x_0(t) & \text{, symbol "0" is transmitted} \end{cases} \tag{2.13}$$

The demodulation can be coherent and non-coherent. The coherent demodulation can be seen as a correlator, where the receiver does contain copies of the chaos generator system information ($x_1(t)$ and $x_0(t)$). Depending on the transmitted signal, one of these copies will synchronized with the received

signal and the the other will be de-synchronized at the receiver. Hence, the match/mismatch will tell about the transmitted information bits.

As for non-coherent receivers, it is required that the transmitted chaotic signals should have different bit energies (i.e., different levels for information bits "1" and "0"). Thus, by comparing the bit energy with a decision threshold (works like a matched filter), we can easily recover the transmitted original information bits. Moreover, [53] reports that some non-coherent schemes can exploit the distinguishable property of a chaotic generator for demodulation process. In particular, if the two chaotic signals come from the same system with different bifurcation parameters, demodulation can be performed by estimating the bifurcation parameter of the "reconstructed" chaotic signal.

Chaos On Off Keying (COOK)

Chaos on off keying works similar to chaos shift keying, but instead of sending two different chaos signals, the chaos on off keying modulator works like an on-off switch whose state depends on the information bits "1" or "0" respectively [52]. For example, when the information bit is "1", the chaos signal $x_0(t)$ is sent, otherwise no signal is sent. This technique provides a higher distance for a given energy per bit E_b between the elements of an information signal set. This scheme is suitable for indoor wireless applications [54]. The transmitted signal is given by

$$s(t) = \begin{cases} x_0(t) & \text{, symbol "1" is transmitted} \\ 0 & \text{, symbol "0" is transmitted} \end{cases} \tag{2.14}$$

Differential Chaos Shift Keying (DCSK)

The differential chaos shift keying was introduced in [55] and shows to outperform CSK schemes when the channel condition is so poor that it is impossible to achieve chaotic synchronization. This modulation scheme is similar to that of the differential phase shift keying (DPSK) except that the transmitted signal is a chaotic - generated signal. In DCSK modulation, each transmitted symbol duration is divided into two identical time slots. The first time slot serves as a reference while the second slot carries the information. If bit "1" is to be sent, the chaotic reference signal (in first slot) is repeated in the second slot; if bit "0" is to be sent, an inverted copy of the reference signal (in first slot) will be sent. Hence, the transmitted signal for information bit "1" is given by

$$s(t) = \begin{cases} x_0(t) & \text{for}(l-1)T_b \leq t < (l-1/2)T_b \\ x_0(t - T_b/2) & \text{for}(l-1/2)T_b \leq t < lT_b \end{cases} \tag{2.15}$$

if the information bits is "0",

$$s(t) = \begin{cases} x_0(t) & \text{for}(l-1)T_b \leq t < (l-1/2)T_b \\ -x_0(t - T_b/2) & \text{for}(l-1/2)T_b \leq t < lT_b \end{cases} \tag{2.16}$$

At the receiver the two received signals are correlated and the decision is made by a zero threshold comparator. The biggest drawbacks of DCSK are the E_b is double and the symbol rate is halved. However, it also offers several advantages over CSK in high noise channel environments. DCSK does not require synchronization and is not sensitive to channel distortion as some other coherent methods are; this is so since both the reference signal and the information signal pass through the same channel.

Chaos CDMA

Conventional CDMA spread spectrum has an explosive impact on our daily personal communications. The CDMA system can be seen in our daily communication devices, especially in third generation (3G) mobile systems, where it aims to provide us with the ability to use voice and data services between the mobile terminals. In order to provide these services, we must provide an efficient radio link that provides high-frequency, low-power and multiple access communication, where every user appears as white noise signal to all other users using the same link. To do so, we can either spread each symbol using a pseudo random sequence to increase the bandwidth of the transmitted signal, or represent each symbol by a piece of "noiselike" waveform. Hence, the chaos noise generator can be used.

The properties of chaotic signals suitable for CDMA have been widely studied and shown to provide advantage over the conventional methods of generating the spreading code sequence [44, 45, 46, 47]. The natural property of chaotic signals that produces a bifurcation behavior makes it possible to generate "noise-like" signals, theoretically and practically. In the conventional noise generator, the pseudo random generator or specially designed CDMA code sequence is produced by visiting each state of the system once in a deterministic manner. With only a finite number of states to visit, this sequence is necessarily to be periodic. On the other hand, the chaotic system in theory has an infinite number of analog states and therefore produces an output sequence which never repeat itself. Hence, exploiting the random, noise-like and aperiodic properties of chaos theory makes it possible to use chaos in generating a new class of CDMA code sequences.

2.1.4 Other Applications

Chaos is always around our world and is found in all disciplines across the board. Such examples include the weather behaviour, biomedical signals (include brain and heart), laser systems, electronic circuits, chemical reactions, mechanical systems, financial data, and all other areas that we can think of.

Chemistry and Chemical Engineering

In a chemical reaction, chaos can be very useful to minimize the energy required in mixing two fluids thoroughly [56]. In chemical applications, there are not many control parameters to be used as compared to electrical and electronic applications. Typical variables are the input flow rates, overall temperature, or concentration of a chemical. In other words, the better the control of mixing of two chemicals (input flow rates), the better their performance is. A good mixing method using chaotic mixing is therefore much faster and more efficient than those using diffusion processes. This can also be seen in combustion applications where chaos can also enhances the mixing of air and fuel. Chaotic mixing in heating can also be applied in plasma heating for a nuclear fusion reactor in heat wave injection. [57]

Mechanical Systems

Vibration in mechanical systems could bring a benefit or a destruction depending on its use. Vibration can be periodic, non-periodic, linear, non-linear or a chaos system, hence one that intends to design a vibration equipment could possibly use and benefit from chaos systems. On the other hand, one that intends to have a stable equipment could model the chaos behaviour of the instability

and control it. Techniques of creating or suppressing chaos systems can be seen in washing machines. Just like chemical engineering, the chaotic changes in vibration and rotational speed in washing machines provide a better mixing of the laundry and a better dissolving of the detergent. The use of chaos motion over a periodic rotation system can also be found in drilling and smoothing applications. In drilling technology, a chaotic rotation of a drill proved to provide a smoother surface of a hole than those system utilize a periodic rotation [58].

Electrical Systems

The modern world is highly dependent on electrical energy, hence the stability of electrical power system operation is one of the most crucial issue. Electrical grid distribution on a heavily loaded system that spreads out over large areas could easily cause chaos under certain loading conditions in a simple power system [59, 60]. These failures may be caused by sudden lighting or electricity powered equipment which will result in instability of the whole power system. Hence, studies of the saddle node bifurcation of equilibrium points are carried by [61]. Other studies of electrical breakdown related to chaos can also be found in [62].

Data Coding Applications

Data coding is another interesting area of application where chaos theory could be applied. Numerous reports have been found in related coding theory applications, including audio compression, video compression, public key cryptography systems [63, 64, 65] and channel coding [66].

Optical Communications

While channel conditions for wireless communications can rapidly change, this is not the case in optical communications. In most cases, an optical communication channel is modelled under an additive white Gaussian noise environment. This benefits from chaos modulation while a perfect synchronization is possible under this condition. Thus, chaos modulation has recently been proposed for optical communication systems that are advancing to push the bit rate into the Gb/s region. Chaotic optical communication using optoelectronic feedback systems with chaotic wavelength fluctuation has been proposed [67]. Recently, lots of other promising uses of chaotic modulation are carried out by research in the optical communication arena which can be easily found in literature, e.g., [68, 69, 70].

2.2 Adaptive Algorithms

In communication engineering, statistical signal processing is one of the major parts of a wireless receiver. Even though the impurity of the wireless channel distorts the transmitted signals, the distorted signals still retains their higher-order stochastic properties. Adaptive filtering techniques used to process signals in an environment of unknown statistics are very attractive tools to the communication problem. We can find that adaptive filtering techniques are successfully applied in all kinds of engineering with such diverse fields as biomedical, mechanical, chemical, control, radar, sonar, and communications engineering. Adaptive filtering techniques are used in a wide range of applications in communications, including echo cancellation, adaptive equalization, adaptive noise cancellation, channel estimation, adaptive demodulation and adaptive beam-

forming. These applications involve processing of signals that are generated by systems whose characteristics are not known a priori [71, 72]. Under this condition, a significant improvement in performance can be achieved by using adaptive rather than fixed filters.

The primary feature of an adaptive filter is the ability to self-adjust (or learn) its coefficient according to the system conditions. An adaptive filter uses an iterative (recursive) algorithm (known as adaptation algorithm or adaptive filtering algorithm) to provide a self-designing ability. In a stationary environment, the conventional filter is to be optimum only when the statistical characteristics of the input data match the "a priori" information on which the design of the filters is based [71]. However in an unknown (little or no information) signal case, the adaptive algorithm starts from an initial guess based on the knowledge known to the system, then the system refines the guess in an iterative process, eventually converges to the optimal Wiener solution in some statistical sense. As for non-stationary environment, which is more likely to be the case of wireless signals, conventional filtering methods are not suitable as the channel conditions are always changing; adaptive algorithms offers a tracking capability that can follow the time variations in the statistics. Thurs, it is suitable for wireless communication applications.

A wide variety of adaptive algorithms have been developed in the literature. Depending on their application, adaptive algorithms are chosen based on their performances using the factors listed below [71]:

1. **Rate of convergence.** Look at how fast or how many iterations are required before an adaptive algorithm converge to the optimum Wiener solution in the mean-square sense. Fast convergence is essential in wireless communication.

2. **Misadjustment.** This quantity describes the steady-state behavior of the algorithm and measures whether the averaged final value of the mean-squared error exceeds the minimum mean-squared error produced by the optimal Wiener filter.
3. **Tracking.** As the name suggests, the tracking ability of the adaptive algorithm is proportionally related to rate of convergence. The algorithm is required to have a good tracking behaviour to track statistical variation in the wireless channel conditions.
4. **Robustness.** Robustness is another important factor to consider. An adaptive algorithm should be robust to small disturbances that arise from different factors, internal or external. Short-term disturbances or estimation errors will not have much effect on the overall system performance.
5. **Computational requirements.** In mobile devices, computation power is very limited and short computation time is required. Some adaptive algorithms are computationally intensive and hence not suitable for wireless communications. The number of operations required for one complete iteration of the algorithm is normally used for complexity estimation. The amount of memory needed to store the required data and the algorithm itself can also have a big impact on the price and complexity of the device. Hence, fast and less complex algorithms are needed.
6. **Numerical properties.** Quantization error in digital communication is the major cause of numerical instability. The implementation of adaptive algorithms on a digital device which operates using finite word-lengths results in quantization errors. An adaptive algorithm is said to be numerically robust when it is insensitive to variation in the word-length

used in the digital device.

Ideally, we want to have an adaptive algorithm that is numerically robust with high convergence rate and small misadjustment, yet it is simple and low in computational complexity that can be implemented on a digital chip easily. However, these hardly happen and can be contradictory with each other where some kind of trade-off is needed. Hence, careful selection of different adaptive algorithms based on its application is required.

Early work on adaptive filters can be traced back to the late 1950's, where the least-mean-square (LMS) algorithm emerged as a effective, yet simple algorithm devised by Widrow and Hoff in 1959 [71, 72]. The LMS is a stochastic gradient algorithm that iterates each tap-weight of the transversal filter in the direction of instantaneous gradient of the squared error signal, but with a drawback of slow convergence, especially when the input is colored. On the other hand, the well known recursive least squares (RLS) algorithm exhibits faster convergence, but it is very complex and sensitive to numerical problems. In this thesis, the LMS based algorithm is implemented and modified to apply in chaotic signal environment.

2.2.1 Adaptive Applications

Adaptive algorithms have found a variety of applications. Generally, these applications can be classified into four major groups: identification, inverse modelling, prediction, and interference cancelling. Although these different classes of applications are different in nature, the basic building blocks for all these applications are similar, where no significant change is requested and different structures are possible with minimal modification. All four classes do have a

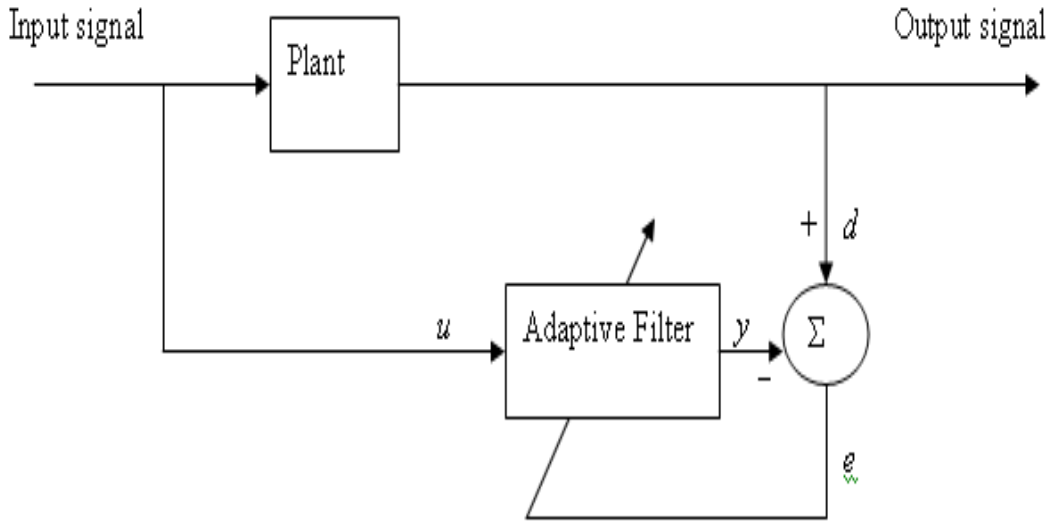

Figure 2.1: Adaptive filtering application configuration: Identification.

common input vector and desired response used to calculate an estimation error. The estimated error is then used to control a set of filter coefficients. Depending on the application and filter design, the adjustable coefficients can be in the form of FIR filter weights, reflection coefficients, antenna array coefficients, rotation parameters, or synaptic weights. All four classes are listed below and the following notations are used in the figure [71, 72]:

$$
\begin{aligned}
u &= \text{input applied to the adaptive filter} \\
y &= \text{output of the adaptive filter} \\
d &= \text{desired response} \\
e &= d - y = \text{estimation error}
\end{aligned}
$$

1. **Identification.** Figure 2.1 shows a block diagram for the adaptive al-

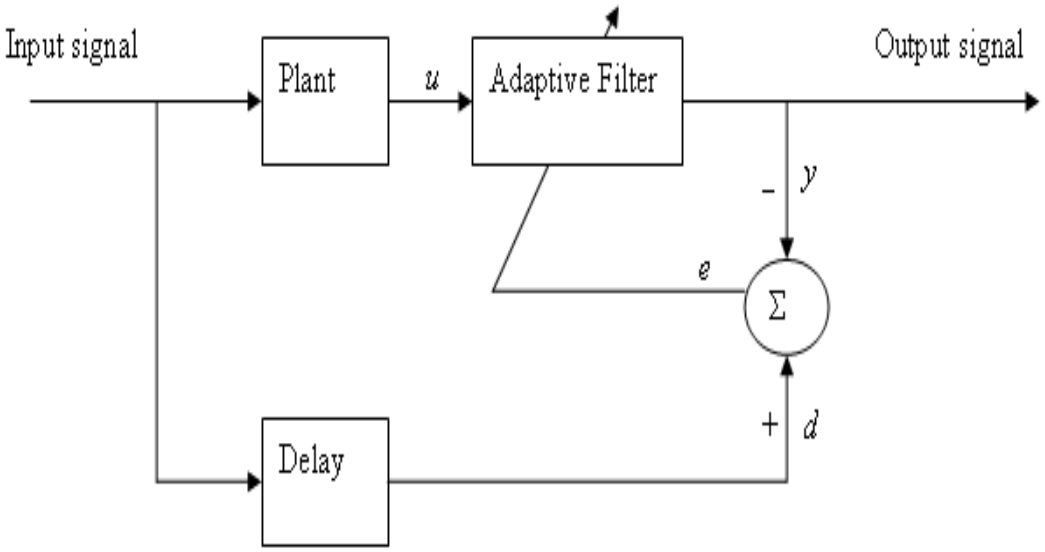

Figure 2.2: Adaptive filtering application configuration: Inverse Modeling.

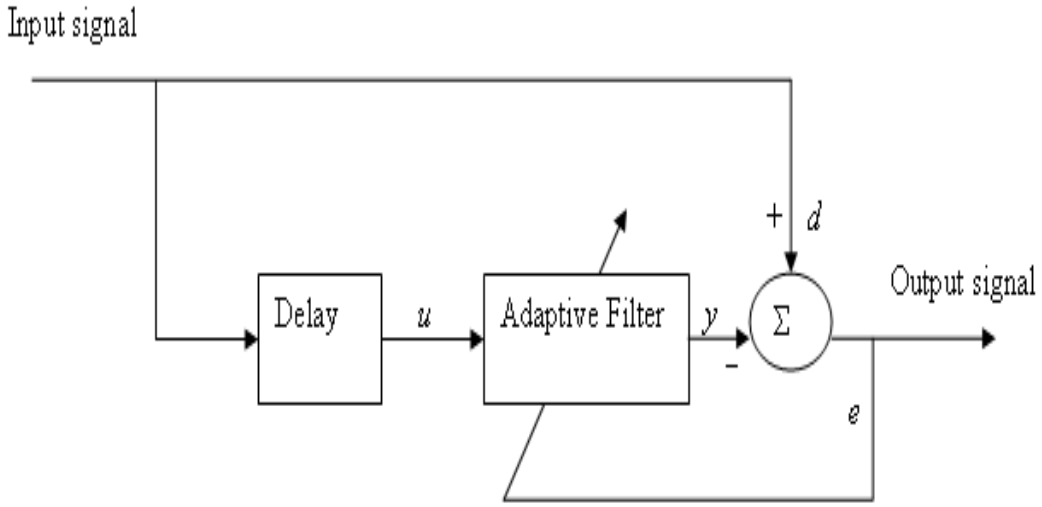

Figure 2.3: Adaptive filtering application configuration: Prediction.

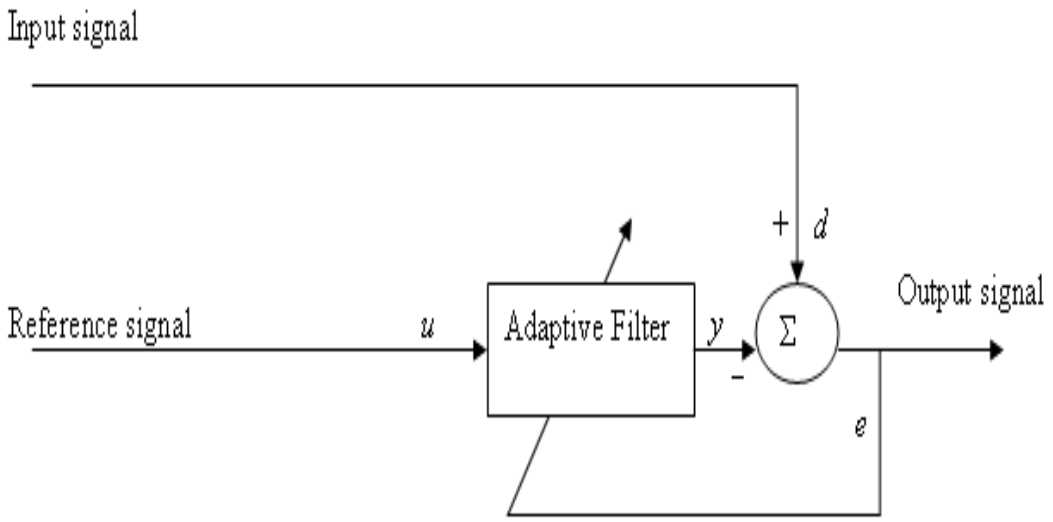

Figure 2.4: Adaptive filtering application configuration: Interference cancellation.

gorithm application class: identification. This configuration provides a linear model that represents an unknown plant. If the unknown plant is dynamic in nature (similar to wireless channel), the model will be time-varying, hence suitable for channel estimation in wireless communication.

2. **Inverse modeling.** Figure 2.2 shows a block diagram for adaptive algorithm application class: inverse modelling. Similar to identification, the inverse modelling configuration provides an inverse version to represent an unknown plant. In digital communications, this is used for adaptive equalization to combat ISI and some thermal noise generated by the receiver at its front end.
3. **Prediction.** Figure 2.3 shows a block diagram for the adaptive algorithm application class: prediction. Here the function provides the best fit prediction of the present value of a random signal or unknown plant.

The system can be used in the area of adaptive demodulation, signal detection, and adaptive pulse-code modulation.

4. **Interference cancellation.** Figure 2.4 shows a block diagram for the adaptive algorithm application class: interference cancellation. A reference signal is used to supply the input signal when the information-bearing signal component is weak or is undetectable. Adaptive noise reduction, echo cancellation and adaptive beamforming applications utilize this configuration scheme.

In the literature, adaptive applications have been proposed in digital communications for a variety of applications. For chaos communications, adaptive algorithms are reported to be used for adaptive demodulation [40, 41, 73, 74]. Channel estimation and echo cancellation using an adaptive algorithm in chaotic coded signal environment are also shown in [75]. Adaptive identification and equalization in chaotic communications are presented in [76]. In this thesis, we conducted a study on the use of adaptive algorithms in chaos communication, particularly for adaptive multiuser detection, adaptive beamforming, and adaptive noise reduction in chaos signals.

2.3 Conclusions

Understanding chaotic signals and their application is only a recent advancement in science. It was virtually unknown to science where chaos to be applied. It is only within the last three decades that much progress has been made and provided some understanding of many concepts related to chaos which began to gain acceptance in the scientific community. Although there are still a lot of technical difficulties in chaos applications, significance of future applications

drive scientific research to persevere in understanding chaos. On the other hand, adaptive algorithms have been shown to provide promising tools and applications for wireless communications. The study of adaptive algorithms for chaotic signals is essential and could possibly lead to further performance enhancement in chaos communications. Hopefully within a short time and with the help of different signal processing tools such as adaptive algorithms, secure chaos communications and many other chaos applications will be put in practical use.

In this chapter, some basic knowledge in chaos have been introduced. Different types of simple chaos generators are introduced and the application of chaos in different engineering arenas is briefly handled. The application of chaos particularly in wireless communication is very appealing. Different types of chaos schemes for wireless communications are introduced. A brief introduction to adaptive algorithms and their possible applications is also presented.

Chapter 3

Secure Chaos Communication and It Applications

3.1 Introduction

The analysis of any dynamic system may be considered as a non-linear behavioral problem. One of the easiest ways to model a dynamic system is to use a deterministic modelling technique such as Chaos Theory [9]. The application of a chaotic modelling technique is simple yet provides a system behavior that is close to a dynamic non-linear system. Much of this research effort has recently been devoted to the use of Chaos Theory in communication engineering [17, 18, 19, 20, 21, 31, 51, 77, 78]. The non-linear behavior of a chaotic system, in addition to its bifurcation property, are well-suited in enhancing the security performance of existing communication systems. It has also offered several possibilities for new applications and performance enhancements. A review of current literature shows that a chaotic generator exhibits a set of properties which are suitable for use in spread spectrum (SS) communication systems. The basic principle of a spread spectrum system is to extend the original information data over a broad bandwidth of frequencies. To be able to perform

spreading on the information data, the system requires a spreading code or sequence that provides auto- and cross-correlation behaviors similar to those of white noise. In a conventional spread spectrum communication system, a pseudorandom or a pseudo-noise (PN) sequence generator is used to produce the spreading code. Some systems use specially designed codes such as, Gold codes, Kasami codes, Walsh Hadamard, and OVSF codes [79] for spreading the information data. However, one of the main issues with these types of spreading code generators is that they suffer from the 'periodicity' problem. This is due to the fact that the generated code sequences have a fixed number of states and the state-machine utilized runs through each sequence in a deterministic manner. It is this periodicity behavior of pseudorandom sequences which compromises the overall security of the system. Moreover, it reduces the system capacity [9]. In contrast, a chaotic generator can produce these noise-like sequences in a non-repeating fashion [19, 20, 21, 78]. A chaotic generator can be considered as an unlimited state-machine. Therefore, it can produce non-repeating sequences which are non-deterministic. This non-periodic behavior of chaotic generators offers significant advantages over the conventional pseudo-noise based SS systems in terms of security, synchronization, and system capacity. Since the solution of the synchronization offered by Pecora and Carroll in 1990 [31], there have been an increasing number of proposed schemes that utilize chaos theory in SS communication systems. Such schemes include but are not limited to: chaotic masking, analog chaos modulation, digital chaos modulation (e.g., Chaos Shift Keying), and Chaotic CDMA sequences [17, 18, 19, 20, 21, 31, 51, 77, 78]. On the other hand, the demand for multimedia applications and services over fixed-line and wireless networks such as short range SS communication and 3G mobile communication systems has grown considerably. Reported studies into

next-generation (NG) wireless/ mobile networks [80] have shown a significant trend towards personalized mobile/ wireless communications and a stronger need for highly-secured wireless multimedia-equipped devices. This trend has stimulated a significant increase in the amount of transmitted data due to the multimedia content, causing a major shift from traditional wired telephony-oriented services which have predominantly supported the transmission of voice data.

It is well known, however, that one of the main issues with multimedia communication is the degradation in communication channel performance, system latency, and acceptable quality of multimedia data received on communication terminals/ devices. This is mainly due to the inherent characteristics of wired or wireless communication systems - e.g., the time-varying nature of wireless channel conditions and the propagation environments [81].

Despite the ongoing development of key communication technologies to deal with multimedia applications (such as adaptive compression [82] and adaptive modulation and coding [83]), the transmission of multimedia data over wireless communication channels still introduces significant bottlenecks. This is mainly due to the fact that representing multimedia data (such as digital audio/ image/ video) requires a large amount of information, which requires broad bandwidth, high computational load, and a large amount of transmitted power. The communication bandwidth available to wireless/ mobile systems for the transmission of multimedia data are often severely limited, so are the processing capabilities of the communication system/ devices. Mobile radio channels must therefore transmit user information in a highly compressed form, while making efficient use of available frequency spectrum and communication power. As a result, new ways of transmitting multimedia data have become essential

in dealing with the problems associated with wireless multimedia communication. The primary aim, therefore, of this effort to use a chaos approach for multimedia applications is to develop a communication technique that provides a secure channel (guarded from interception) for the transmission of multimedia data with a high spectral efficiency and improved system capacity. Unlike other spreading codes and sequences, it is very difficult to predict a long-term chaotic pattern or sequence even when the fundamental chaotic generator is known to an attacker/ eavesdropper. Even a small error in the estimation of the initial condition used by the interceptor will lead to a very different chaotic sequence and white noise like auto- and cross correlation properties. Hence, it can be shown that it is virtually impossible to intercept information if the exact initial condition of the chaotic generator is not known. In this paper, we propose a modified logistic chaotic map for CSK spread spectrum communication in the application of 'real' multimedia data. This is compared with two different widely-used logistic chaotic maps. Subsequent sections of this paper have been divided as follows: Section 3.2 provides an overview of the Chaos Shift Keying (CSK) modulation technique; Section 3.3 formulates CSK theoretical performance; Section 3.4 provides two commonly-used chaos generators with a modified chaos generator for CSK; Section 3.5 provides multimedia performance results using CSK; Section 3.6 discusses the security aspects of the CSK system. Concluding remarks are presented in Section 3.7.

3.2 Chaos Shift Keying (CSK)

Spread spectrum communication is produced by directly multiplying the information bits (in the time domain) with a known spreading sequence running

at a much higher rate, in order to spread the information over the bandwidth of the transmitted signals. The spreading sequence can be generated using a pseudorandom noise generator or some other specially-designed code generator. However, these generators produce repeating sequences and lead, in a long period of time, to a very predictable fashion which reduces the system capacity and security. To provide a secure communication channel, a chaos generator can be used to generate Chaos Shift Keying (CSK) sequences, where a different sequence can be generated using a different initial condition. Due to its bifurcation behavior, the chaotic sequence is very sensitive to the initial condition chosen. An exact value must be known in the receiver side to be able to demodulate the transmitted CSK signal.

Chaos Shift Keying modulation uses a pair of chaotic sequences (g_1 and g_2) with different bit energies to transmit the binary information [51, 77]. if the l^{th} data bit which occupies the l^{th}-bit period is $\alpha_l = +1$, then g_1 sequences is radiated from the transmitter, while for $\alpha_l = -1$, g_2 sequence is transmitted. The number of chaotic symbols transmitted for one data bit is dependent on the spreading factor (2β) [17]. The output of the CSK transmitter can be written as

$$s_k = \alpha_l g_{v,k} \tag{3.1}$$

where v decides which chaos sequence is to be sent.

The chaotic sequence for CSK g_1 and g_2 can be generated in three different ways. First method: it uses two different chaotic generators. Second method: generating the two sequences using different initial conditions of the same chaotic generator. And the last method: the two sequences are generated by the same chaotic generator with the same initial condition but multiplied by

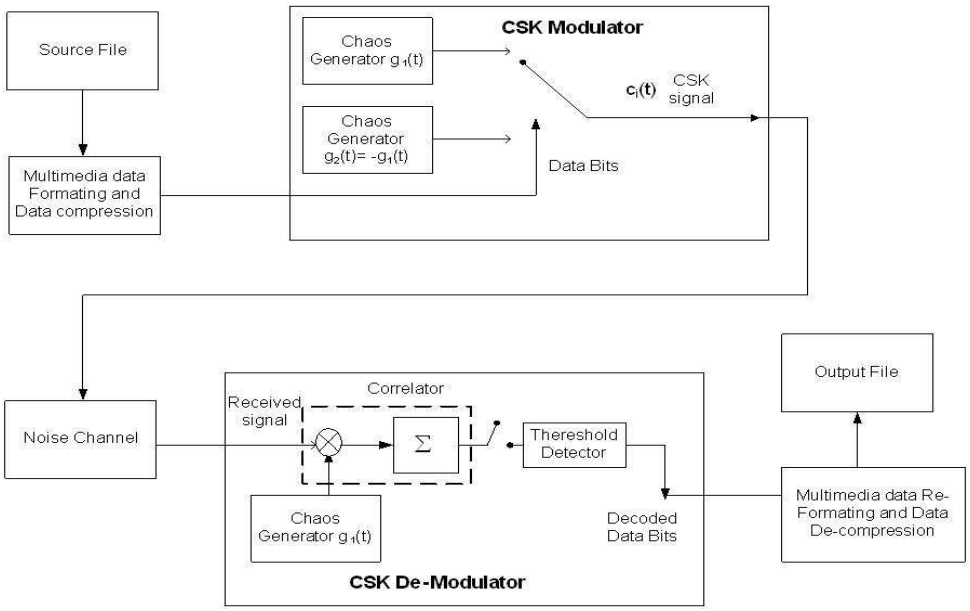

Figure 3.1: A Framework for the CSK communication system.

two different constants. For simplicity, we used the last method to generator two chaotic sequences. In this work the two chaotic sequences are related as $g_2 = -g_1$. And assumed we are only dealing with binary system, where the sign of the binary signal is used to determine the chaotic sequences, hence, the transmitter CSK signal from equation 3.1 can be simplify to

$$s_k = \alpha_l g_k \tag{3.2}$$

The demodulation process is a simple coherent correlator at the receiver as shown in Fig. (3.1)

3.3 CSK Theoretical Background

The performance of the CSK system in an AWGN environment can be derived following the method used in [17, 18]. For a correlator type of receiver, the correlator output for the l^{th} bit y_l is given by

$$y_l = \sum_{k=2\beta(1-l)+1}^{2\beta l} r_k g_k \tag{3.3}$$

where $r_k = s_k + \eta_k$ is the received signal in an AWGN environment during the k^{th} chip period, η_k being additive Gaussian white noise. Now we have:

$$y_l = \alpha_l \sum_{k=2\beta(1-l)+1}^{2\beta l} g_k^2 + \sum_{k=2\beta(1-l)+1}^{2\beta l} \eta_k g_k \tag{3.4}$$

The first term is the required signal and second term is noise. According to the Central Limit Theorem, if we consider a sum of a large number of random variables in the system, we can assume that the system to follow a normal distribution. Hence the BER for the CSK can be formulated as follows:

$$\begin{aligned} \mathrm{BER}_{CSK} &= \mathrm{Prob}(\alpha_l = 1) \times \mathrm{Prob}(y_l \leq 0 \mid \alpha_l = 1) \\ &+ \mathrm{Prob}(\alpha_l = -1) \times \mathrm{Prob}(y_l > 1 \mid \alpha_l = -1) \\ &= \frac{1}{4}\left[\mathrm{erfc}\left(\frac{\mathrm{E}[y_l \mid (\alpha_l = +1)]}{\sqrt{2\mathrm{var}[y_l \mid (\alpha_l = +1)]}}\right)\right. \\ &\left. +\mathrm{erfc}\left(\frac{-\mathrm{E}[y_l \mid (\alpha_l = -1)]}{\sqrt{2\mathrm{var}[y_l \mid (\alpha_l = -1)]}}\right)\right] \end{aligned} \tag{3.5}$$

From [17, 18], the variance of $y_l|(\alpha_l = +1)$ equals to the variance of $y_l|(\alpha_l = -1)$ and we have $\mathrm{E}[y_l|(\alpha_l = +1)] = -\mathrm{E}[y_l|(\alpha_l = -1)]$, where E is the expectation

function. Hence, equation (3.5) can be simplified to:

$$\begin{aligned} \mathrm{BER}_{CSK} &= \frac{1}{4}\left[\mathrm{erfc}\left(\frac{\mathrm{E}[y_l \mid (\alpha_l = +1)]}{\sqrt{2\mathrm{var}[y_l \mid (\alpha_l = +1)]}}\right)\right. \\ &\quad \left. + \mathrm{erfc}\left(\frac{\mathrm{E}[y_l \mid (\alpha_l = +1)]}{\sqrt{2\mathrm{var}[y_l \mid (\alpha_l = +1)]}}\right)\right] \\ &= \frac{1}{2}\left[\mathrm{erfc}\left(\frac{\mathrm{E}[y_l \mid (\alpha_l = +1)]}{\sqrt{2\mathrm{var}[y_l \mid (\alpha_l = +1)]}}\right)\right] \end{aligned} \tag{3.6}$$

where erfc(.) is the complementary error function defined as

$$\mathrm{erfc}(\psi) \equiv \frac{2}{\sqrt{\pi}} \int_{\psi}^{\infty} e^{-\lambda^2} d\lambda. \tag{3.7}$$

The mean value of y_l when $\alpha_l = +1$ in equation (3.4) is given as

$$\mathrm{E}[y_l|\alpha_l = +1] = \sum_{k=2\beta(1-l)+1}^{2\beta l} \mathrm{E}[g_k^2] + \sum_{k=2\beta(1-l)+1}^{2\beta l} \mathrm{E}[g_k][\eta_k] \tag{3.8}$$

We Know that the mean of AWGN is zero, i.e., $\mathrm{E}[\eta_k] = 0$. So the mean for equation (3.8) can be simplified to:

$$\mathrm{E}[y_l|\alpha_l = +1] = 2\beta P_s + 0 \tag{3.9}$$

where $P_s = \mathrm{E}[g_k^2]$ is the average power of the chaotic signal.

As for the variance of y_l in equation (3.4), we know that from [17, 18] that

$$\begin{aligned} 2\text{cov}\left[\sum_{k=2\beta(l-1)+1}^{2\beta l} g_k^2, \sum_{k=2\beta(l-1)+1}^{2\beta l} \eta_k g_k\right] &= 0 \\ \text{var}\left[\sum_{k=2\beta(l-1)+1}^{2\beta l} \eta_k g_k\right] &= \beta N_o P_s \\ \text{var}\left[\sum_{k=2\beta(l-1)+1}^{2\beta l} g_k^2\right] &= 2\beta\Lambda \end{aligned}$$

,where $\Lambda = \text{var}[g_k^2]$. Hence, the variance of y_l when $\alpha_l = +1$ for equation (3.4) is given as:

$$\begin{aligned} \text{var}\left[y_l \mid \alpha_l = +1\right] &= 2\text{cov}\left[\sum_{k=2\beta(l-1)+1}^{2\beta l} g_k^2, \sum_{k=2\beta(l-1)+1}^{2\beta l} \eta_k g_k\right] \\ &+ \text{var}\left[\sum_{k=2\beta(l-1)+1}^{2\beta l} \eta_k g_k\right] \\ &+ \text{var}\left[\sum_{k=2\beta(l-1)+1}^{2\beta l} g_k^2\right] \\ &= 0 + \beta N_o P_s + 2\beta\Lambda. \end{aligned} \tag{3.10}$$

substituting (3.9) and (3.10) to (3.6), the BER for CSK can be found as follows

$$\begin{aligned} \mathrm{BER}_{CSK} &= \frac{1}{2}\mathrm{erfc}\left(\frac{2\beta P_s}{\sqrt{4\beta\Lambda + 2\beta N_o P_s}}\right) \\ &= \frac{1}{2}\mathrm{erfc}\left(\frac{1}{\sqrt{\frac{\Lambda}{\beta P_s^2} + \frac{N_o}{E_b}}}\right) \\ &= \frac{1}{2}\mathrm{erfc}\left(\frac{1}{\sqrt{\left(\frac{E_b^2}{4\beta\Lambda}\right)^{-1} + \left(\frac{E_b}{N_o}\right)^{-1}}}\right) \end{aligned} \tag{3.11}$$

where $E_b = 2\beta P_s$. Equation (3.11) shows that the BER performance can be improve by either reducing Λ (variance of g_k^2), increasing the spreading factor (2β), or increasing the signal power P_s (the $\mathrm{E}[g_k^2]$).

3.4 Some Chaotic Sequences and Their Performance

Two commonly used chaotic generators and our propose modified chaotic generator are studied in this section. To obtain the BER performance for each chaos logistic map or sequence, the signal power P_s and the variance Λ are either calculated from their invariant probability density function (pdf) or numerically obtained from simulation.

3.4.1 Logistic Chaos Generator 1 (LCG1)

This is one of the simplest chaos logistic maps used in generating chaotic sequences for digital communication [17, 18, 19] in which:

$$g_{n+1} = 1 - 2g_n^2 \tag{3.12}$$

with the invariant probability density function given in [17, 18, 19, 78] as follows:

$$\rho(g) = \begin{cases} \frac{1}{\pi\sqrt{1-g^2}} & \text{, if } \mid g \mid < 1 \\ 0 & \text{, otherwise} \end{cases} \tag{3.13}$$

Hence, the values of P_s and Λ for LCG1 can be mathematically calculated using its invariance probability density function as shown by [17]:

$$P_s = \mathrm{E}[g_k^2] = \int_{-\infty}^{\infty} g^2 \rho(g) dg = \int_{-1}^{1} g^2 \frac{1}{\pi\sqrt{1-g^2}} dg = \frac{1}{2} \tag{3.14}$$

$$\Lambda = \mathrm{var}[g_k^2] = \mathrm{E}[g_k^4] - \mathrm{E}^2[g_k^2] = \int_{-1}^{1} g^4 \rho(g) dg - \frac{1}{4} = \frac{1}{8} \tag{3.15}$$

3.4.2 Logistic Chaos Generator 2 (LCG2)

Another dynamic system that is capable of exhibiting chaotic properties for spreading spectrum communication is proposed in [20, 21] in which:

$$g_{n+1} = a g_n (1 - g_n) \tag{3.16}$$

where a is the bifurcation parameter (or control) parameter, which is considered to be in the interval of $3.57 < a \leq 4$; for a non-period chaos system.

In this work, the bifurcation parameter is identified as the 'security key'

of the system. This security key can only be known to the authorized user. Without this key the transmitted signal cannot be demodulated. However, a drawback of this system is that the output of the above sequence lies in the interval $0 \leq g_n \leq 1$, which decreases P_s and increases Λ (as compared to LCG1). This will lead to a lower BER performance. The probability density function for this system is not provided. Numerical simulation is used to obtain, $P_s = \frac{3}{8}$, and $\Lambda = 1\frac{1}{3}$, when $a = 4$. To Increase the system performance, a modified version of this logistic is proposed in the next Section and shown to have a higher value of P_s and a lower value for Λ .

3.4.3 A Proposed Logistic Chaos Generator 3 (LCG3)

The proposed chaos generator (LCG3) in this section is a modification of the logistic chaos generator 2 (LCG2), which is a scaled and shifted version of LCG2. Scaling and shifting the chaos sequence will not change the chaotic properties of the generator but will provide an increase in P_s and a decrease in the Λ value. This will improve the BER performance over LCG2. The proposed logistic chaos generator is as shown below:

$$\begin{aligned} g_{n+1} &= a g_n (1 - g_n) \\ j_{n+1} &= 2(g_{n+1} - 0.5) \end{aligned} \tag{3.17}$$

where j_n is the output chaotic sequence for CSK modulator and a is the chaotic or security parameter, as discussed previously, and is considered to be in the interval $3.57 < a \leq 4$. Again, the probability density function for this system is not provided. Numerical simulation is used to obtain P_s and Λ; which are shown in Table 3.1.

Table 3.1: Statistics of M - Logistic Map 2

a	$\mathrm{E}[g_k^2]$ or P_s	Λ
4	$\frac{1}{2}$	$\frac{1}{8}$
3.97	$\frac{9}{20}$	0.111
3.95	0.410	$\frac{1}{10}$
3.90	0.392	0.095

It should be noted, that when $a = 4$ both LCG1 and LCG3 provide the same values for P_s and Λ. From Table 3.1, we can see that LCG3 can provide the same performance as LCG1 and yet provide improved security by simply changing the security parameter.

3.4.4 Performance of the CSK System

Using equation (3.11), the theoretical BER performance of the CSK system can be plotted against Eb/No as shown in figures (3.2, 3.3, 3.4, 3.5).

From the theoretical curves and simulated results shown in figures (3.6 & 3.7), one can clearly see that the performance of CSK in an AWGN channel can be improved by utilizing a higher spreading factor (SF). Comparing LCG1 to LCG3 based on theoretical BER performance, there is not much difference even when the security parameter a is varied. Both theoretical and simulated BER results show that LCG2 performance drops one order of magnitude when a small value of SF is used. Hence, LCG3 can perform as well as LCG1 with the added advantage of an extra security parameter for enhanced secure communication.

Figure (3.8), shows the performance of the CSK for different SF values in a 10 dB AWGN channel. When a large SF value is employed we can virtually see no difference between all three generators. However, when the SF value is small

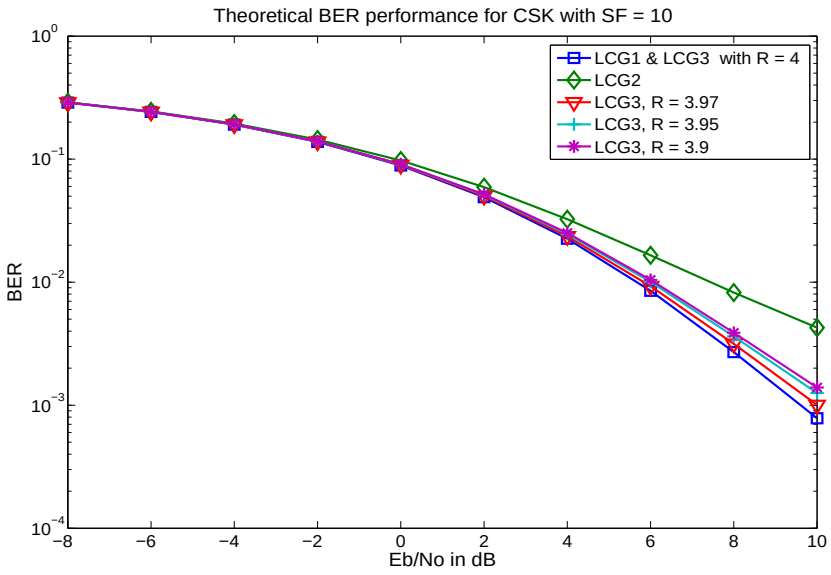

Figure 3.2: Theoretical BER performance of CSK in AWGN Channel with SF=10.

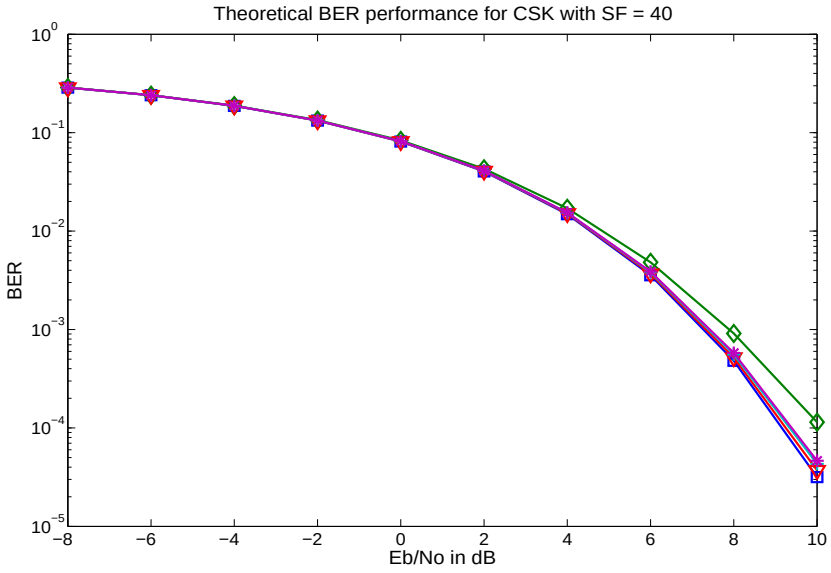

Figure 3.3: Theoretical BER performance of CSK in AWGN Channel with SF=30.

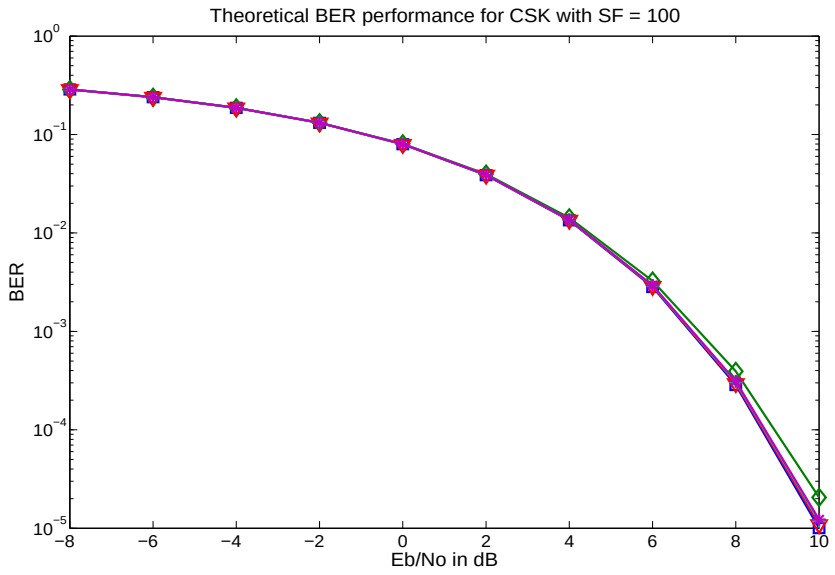

Figure 3.4: Theoretical BER performance of CSK in AWGN Channel with SF=100.

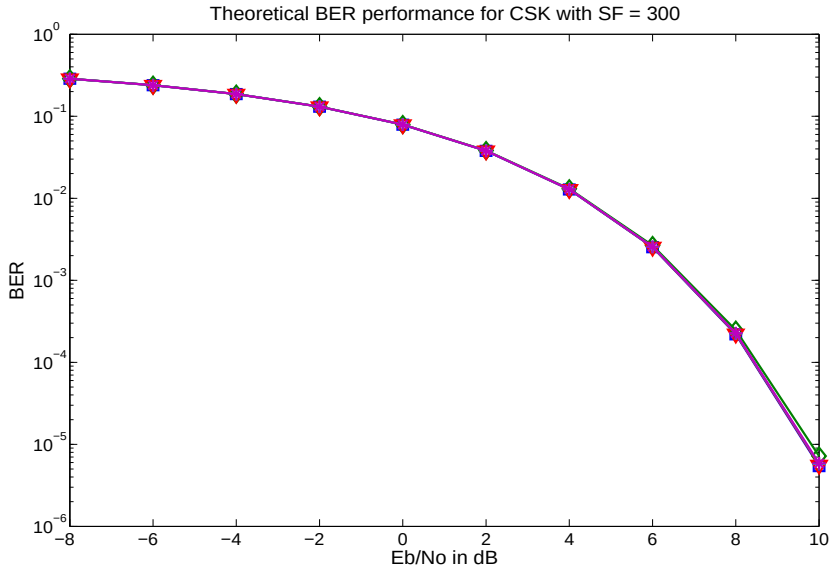

Figure 3.5: Theoretical BER performance of CSK in AWGN Channel with SF=300.

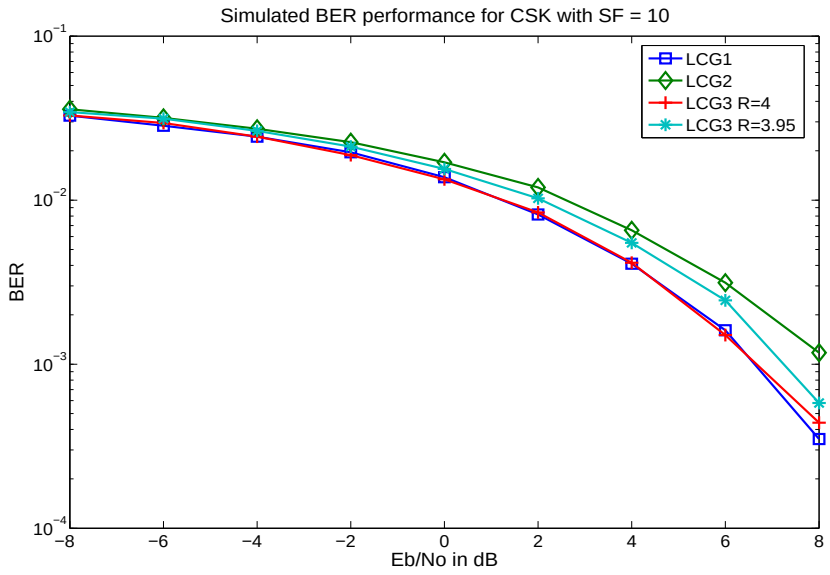

Figure 3.6: Simulated BER performance of CSK in AWGN Channel with SF=10.

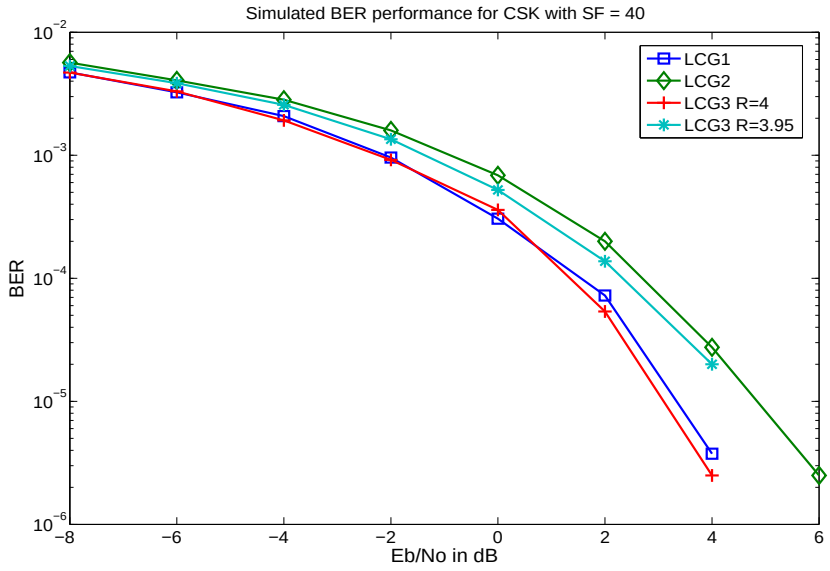

Figure 3.7: Simulated BER performance of CSK in AWGN Channel with SF=40.

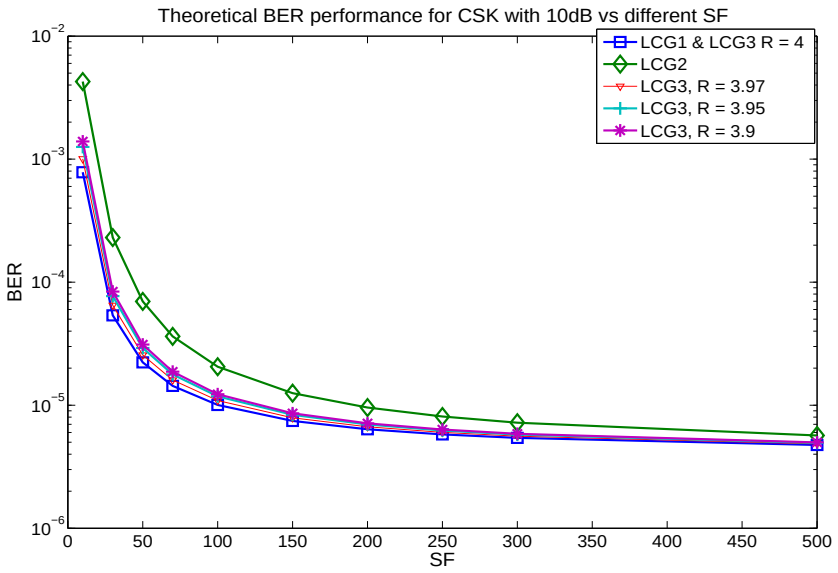

Figure 3.8: Theoretical BER performance of CSK versus different SF with AWGN Channel ($E_b/N_o = 10$ dB).

(around 50 - 100), the BER performance shows a significant difference even for a simple increase in SF value (note: an optimum value of SF for CSK should be around 50 - 100 in an AWGN channel environment).

3.5 Multimedia Framework and Performance Analysis

To enable the simulation of multimedia data over the proposed CSK system, a process for converting multimedia signals from various data sources (such as, compressed audio/ image/ video), which may be stored as files on a PC, has been developed. This has been integrated together with the CSK modulator, to form the overall multimedia simulation framework. A generic transmission

system for multimedia data using the CSK scheme has been implemented using a conversion process which transforms multimedia content to a suitable data format which can be further processed by the CSK modulator.

The principal idea behind the multimedia model developed is to first consider the source data (digitized version of the original multimedia signal with N-bit resolution) as a vector array containing integer quantization levels. For digital audio, these correspond to sampled amplitude values, and for digital image and video coding they correspond directly to pixel values [84]. Before the multimedia information can be processed by the CSK modulator, the source data is converted into a matrix array containing N bit-words which correspond to the sample/pixel levels. Thus, a bit-stream representing the original multimedia data is created. This is subsequently encoded into the required baseband modulated data symbols, as specified by the CSK modulator. In the receiver structure, the reverse functions of the transmitter are performed on the modified data symbols produced by the CSK scheme. Data symbols are first converted back to a bit-stream and are subsequently reconstructed back to the original multimedia data format applied to the system.

3.5.1 Performance Measures

In this chapter, we consider the performance of the CSK system with multimedia data in terms of user (human) perception [84], instead of the traditional BER or MSE performance analysis. These metrics alone cannot be used to determine the overall 'security' of the system and the quality of received multimedia data. Figure (3.9) illustrates the misuse of traditional BER performance over user perceived quality. Figure (3.9) shows that both the shifted image (image pixel is

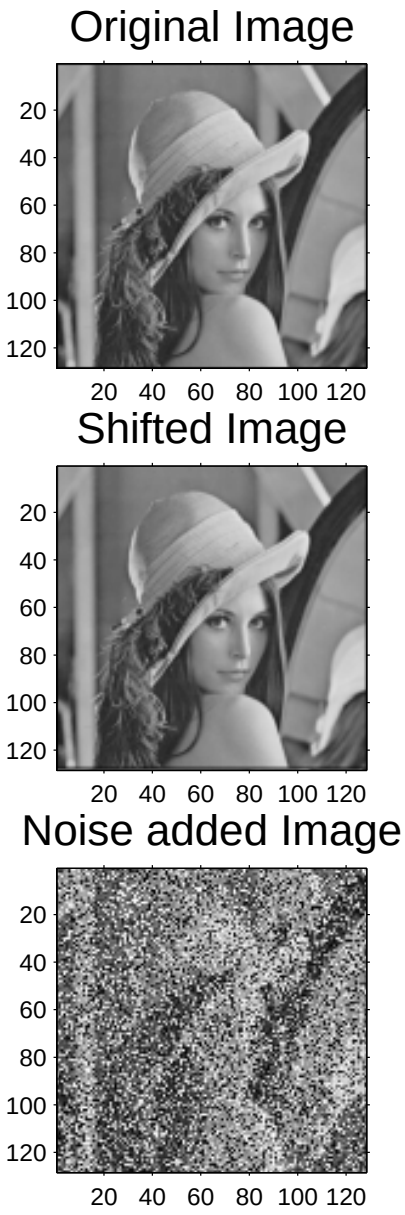

Figure 3.9: Illustrating the misuse of traditional BER performance over user (human) perception.

shifted one line to the top) and the noise-added image (original image with white noise) provide similar BER or MSE measurement, but, perception-wise they are very different from the original Image. Hence, perception-wise performance is important for the analysis of multimedia applications for both secure and non-secure communication. Nevertheless, in a communication system, the BER of the physical channel can provide control over the user-perceived quality (SNR, etc). For digital image applications, for example, the most important quality measure is how the image appears to the end user. This will differ depending on the type of the multimedia content being transmitted, and can be used to ascertain a suitable BER of a particular CSK scheme for the target application.

To evaluate/demonstrate the transmission of multimedia data over a secure communication channel using the proposed CSK system, the simulation framework was configured for the application of still image processing. A standard version of the 512x512 size gray scale Lena image with 8 bits/ pixel resolution [85] was used as the multimedia source data/ file input. Due to practical computational limitations, however, the Lena image was resized to 128x128. Although, this introduces slight imperfections in the image (degradation in visual quality), it has no bearing on the results obtained. The re-sized Lena image used is shown in figure 3.9 (labelled as 'Original Image').

Figures (3.10, 3.11, 3.12, and 3.13) show the performance of different CSK systems for multimedia transmission. On close inspection of the resulting images, we notice that the LCG2 system has a lower performance than the other LCG1 and LCG3 CSK systems. This is confirmed by the theoretical analysis presented in the previous section. However, the difference is small and normally not very noticeable. Although Section 3.4 shows that the three systems provide different BER performance curves, this small variation in BER performance

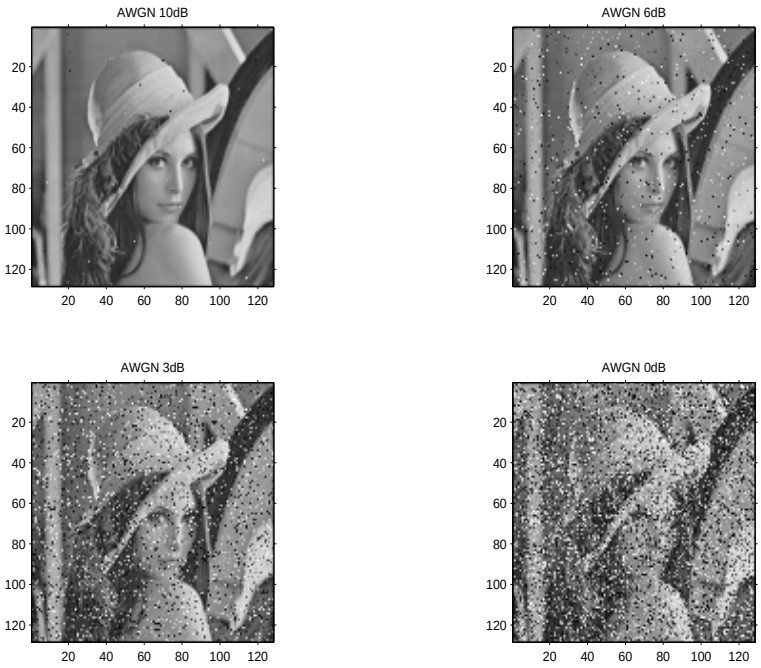

Figure 3.10: Multimedia performance of the LCG1 CSK system in different AWGN environments (SF = 10).

may not be too apparent perception-wise for multimedia applications. Importantly though, it provides means of determining an acceptable E_b/N_o required for a suitable user perceived quality. For an AWGN channel environment, simulation results of the CSK system show that good image quality is maintained generally at a minimum of 10 dB required for E_b/N_o .

3.6 Security Overview

Measurement of the 'security' aspects of any communication system is not an easy task to undertake. However, we can view security in a few different ways.

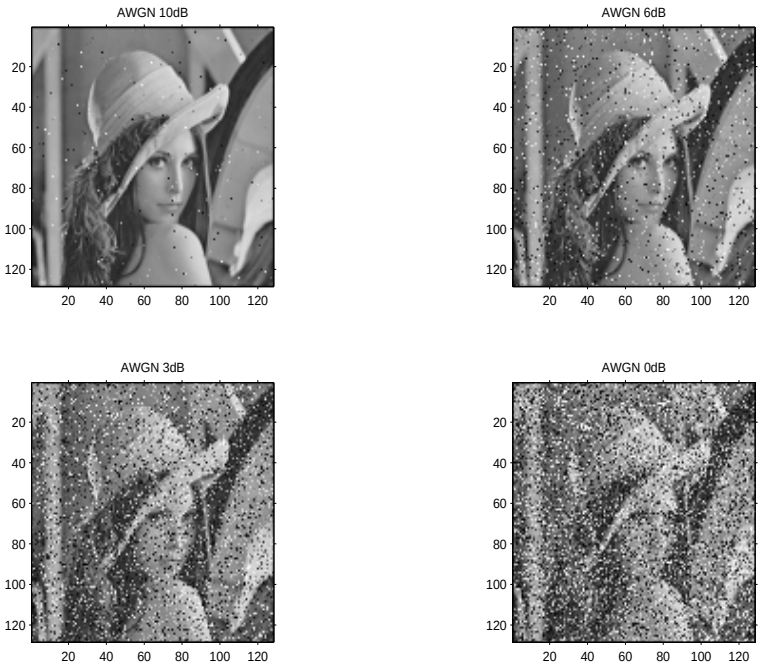

Figure 3.11: Multimedia performance of the LCG2 CSK system in different AWGN environments (SF = 10).

To begin with, the auto- and cross- correlation property is used. This is the simplest security measure for any spread spectrum communication system. If a spreading sequence provides an auto and cross-correlation characteristic not similar to white noise, we can conclude that this would be unsuitable for spread spectrum communication. Also, since there is some correlation between two sequences, it could be easily intercepted by an attacker.

Figures (3.14) and (3.15) show the auto- and cross-correlation performance for all three chaos generators with different values for the initial condition, and the security parameter defined in section 3.4. It is quite evident that LCG1 and LCG3 have auto- and cross-correlation properties similar to those of ran-

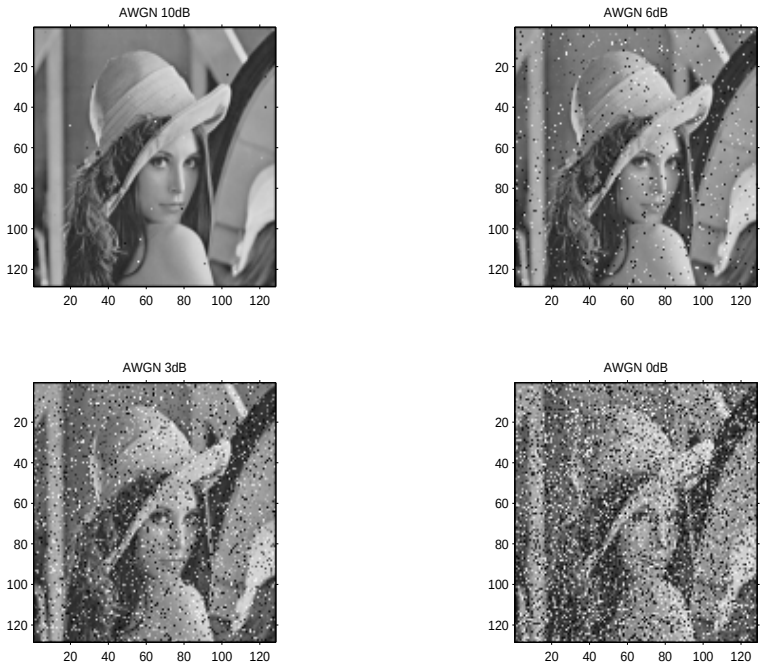

Figure 3.12: Multimedia performance of the LCG3 CSK system in different AWGN environments (a = 4, SF=10).

dom white noise, despite the fact that their initial conditions are just slightly different. This indicates that LCG1 and LCG3 can generate sequences that are uncorrelated. However with LCG3, more security is embedded with its extra security parameter (even small variations in provide uncorrelated sequences). Hence, the generation of a chaos sequence is very sensitive to the initial condition. A slight difference in the initial condition will generate a totally different chaotic sequence.

In the case of an unauthorized attacker trying to gain access to the communication system using LCG3, as compared to LCG1, an attacker would need to know not only the exact initial condition for the chaos generator but also the

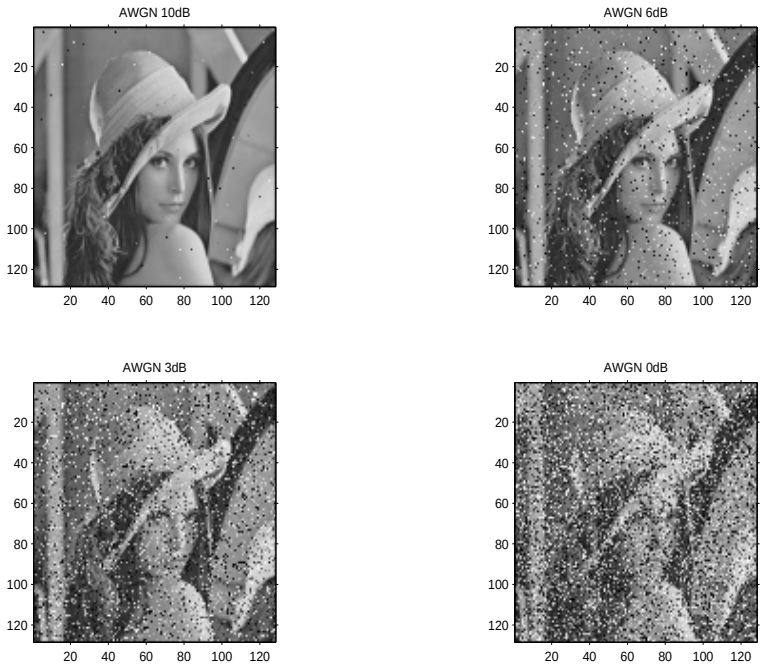

Figure 3.13: Multimedia performance of the LCG3 CSK system in different AWGN environments (a = 3.9, SF=10).

security 'key' (parameter) before interception/demodulation of any information could be possible; even if the sequence generating method was also known to the attacker. This process is fairly similar to other encryption processes where a unique security key is needed. This additional security parameter, therefore, enhances the security performance of the communication physical link.

Figure (3.16) illustrates the orbits generated using two very close initial conditions and two very close security parameters for each chaotic logistic map. More importantly, it shows how fast or how long for a sequence before it is out of the orbit of similarity. Results show that an exact initial condition is needed and that no long-term prediction is possible in all three chaos generators. Figure

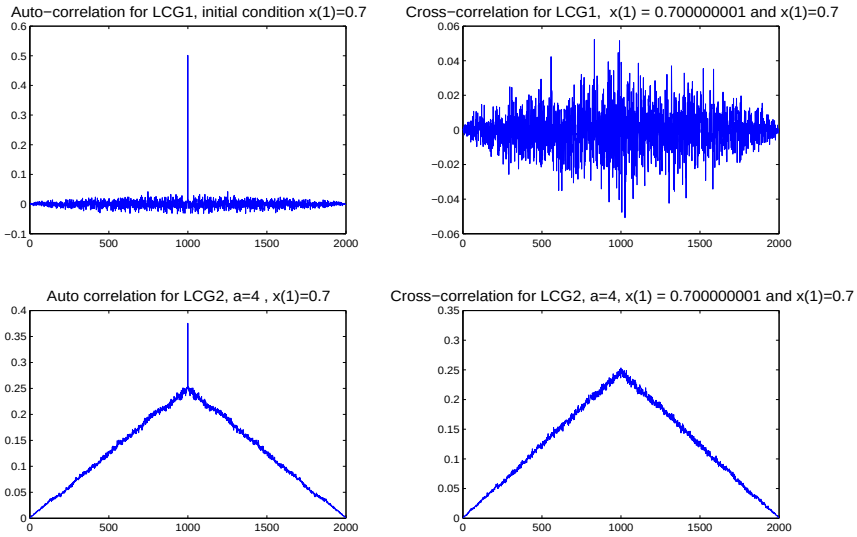

Figure 3.14: Correlation performance for LCG1 and LCG2.

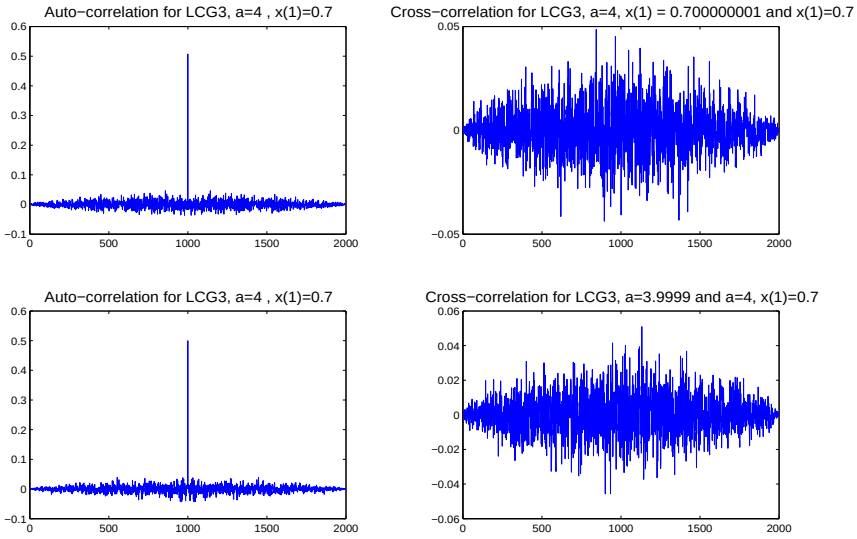

Figure 3.15: performance for LCG3.

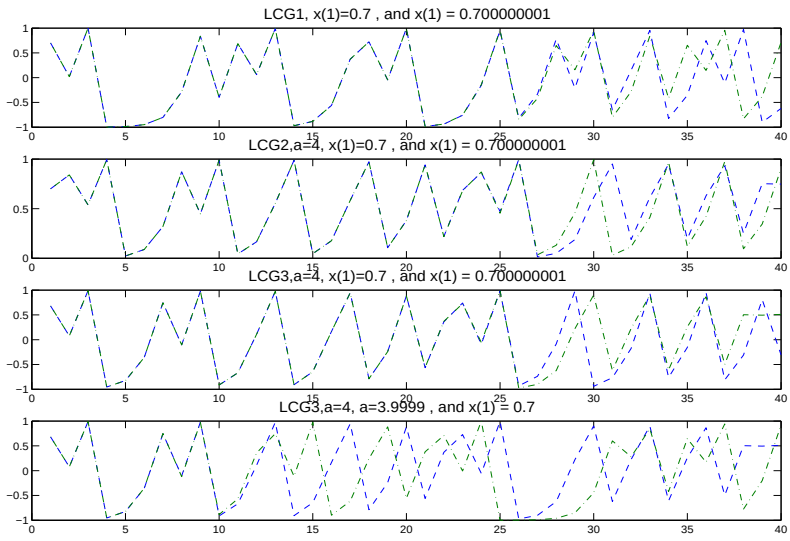

Figure 3.16: Different chaotic sequences generated by each chaotic generator with different initial values and bifurcation parameters.

(3.16) also shows that LCG3 provides the most secure communication, where only 10 iterations are needed (for a different parameter a) before the sequences go off the orbit. In general, all three generators provide a very secure communication channel, as approximately 25 iterations are needed for the sequence to go off the orbit.

The shorter the sequence for SF the more vulnerable it is for the attacker to decipher the transmitted signal. Larger SF can ensure harder prediction of the spreading sequence; hence using chaos generator can ensure higher security to the physical signal due to it bifurcation behaviors. In other words, it is hard to predict or even estimate its chaotic spreading sequence. As a result, it is better to have a larger spreading factor (more than 25) to ensure security [7]. It is recommended in this case to have a SF of 50 to 100 to provide optimum performance.

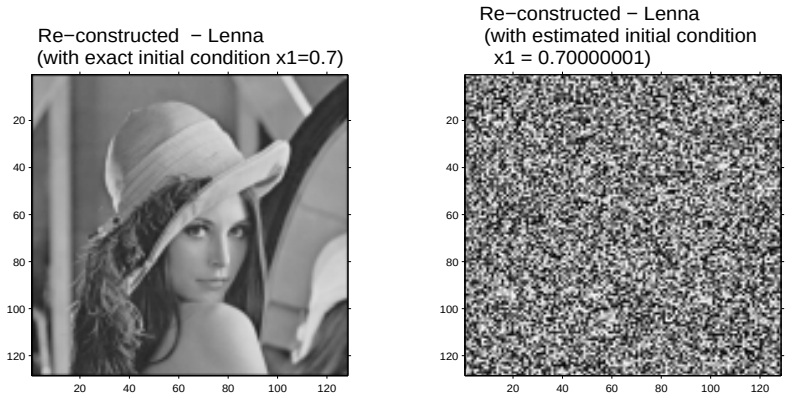

Figure 3.17: Multimedia secure communication using LCG1.

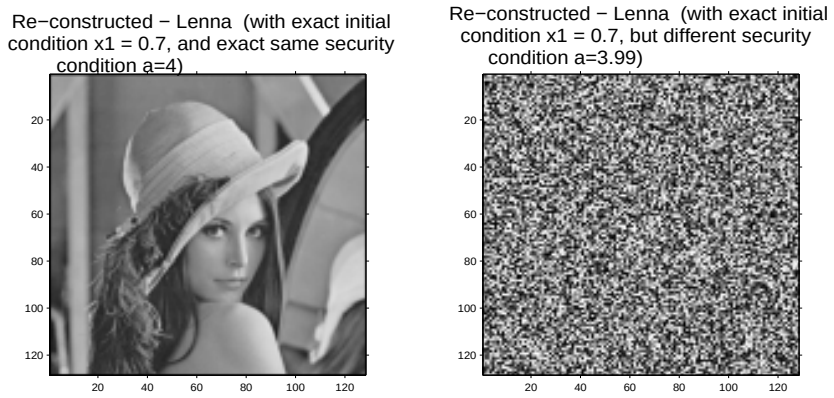

Figure 3.18: Multimedia secure communication using LCG3 with a different security condition (bifurcation parameter).

To illustrate the security performance of CSK using LCG1 and LCG3, the system was simulated with the Lena image by deliberately estimating the initial condition and security parameter a - emulating the process that would otherwise be used by an attacker. Figures (3.17) and (3.18) show the resulting image (error) obtained in estimating the initial sequence for LCG1 and in estimating the security parameter for LCG3 respectively. The demodulated multimedia data (image) for both cases is totally unrecognizable even though the BER of the system is very small (almost 0.05). Hence, we can confirm that the analysis of BER performance data is not suitable in determining the effectiveness of secure communications in the system. Instead, security measurement can be readily extracted from simple observation - human perception. Moreover, figure (3.17) shows the additional level of security achieved in multimedia communication due to the bifurcation property of LCG3

3.7 Conclusion

In this chapter we proposed a modified logistic chaotic map for chaos-shift-keying (CSK) to transmit multimedia data over a highly-secure spread spectrum communication system. This approach was compared with two commonly used logistic chaotic maps. The proposed logistic chaotic map shows BER performance similar to the optimum performance obtained for CSK modulation. Simulation results (based on the application of digital images) and user-perception analysis showed that the additional bifurcation parameter from the proposed logistic chaotic map provides another level of security in spread spectrum communication.

Chapter 4

Space-Time Diversity For Chaos Communication

4.1 Introduction

In today's climate of increased criminal attacks on the privacy of personal or confidential data and with a significant shift in the use of multimedia applications (digital images/video) to convey information over digital communication systems, a high secure physical communication link with an optimum bit-error-rate (BER) performance is required for both wired and wireless communication systems. As stated in chapter 3, Conventional spread spectrum (SS) communication is produced by directly multiplying the information bits (in the time domain) with a known spreading sequence running at a much higher rate, to spread the information over the bandwidth of the transmitted signal. The spreading sequence can be generated using a pseudo-random noise generator or some specially-designed code generator. However, these generators produce repeating sequences and lead to a very predictable fashion which reduces the system capacity and security. Recent research suggested the use of chaos generator to target the security drawback for spread spectrum communication [8, 7].

To provide a secure communication channel, a chaos shift keying (CSK) system is used as described in chapter 3. In order to enhance the error-rate performance of this secure chaos communication, the adaptive transmission scheme proposed in [86] is used. To combine CSK with the adaptive transmission scheme in [86], we first encode the chaos chip-symbols into orthogonal space-time block codewords and transmit these codewords in the eigen-directions of the wireless channel to provide diversity in the spatial domain. In this work, we also investigate the performance improvement from such combination over a macrocell channel model that is originally proposed in [12] and proved to be a realistic model.

This chapter is organized as follows. Section 4.2 describes the general CSK modulation and demodulation technique. Section 4.3 explains the process of orthogonal space-time block code (O-STBC) encoding of chaos chip sequences. Section 4.4 describes the wideband frequency-selective channel and the spatial correlation model that is used in our simulation. Section 4.5 provides an overview of eigen-beamforming technique. Section 4.6 shows the overall system, received signal model, maximum likelihood decoding rule for OSTBC matrices, and simulation results. Conclusion is then delivered in Section 4.7.

Notation used: $(\cdot)^*$, $(\cdot)^T$, and $(\cdot)^H$ are complex conjugate, vector transposition, and Hermitian transposition, respectively. $\|\cdot\|_F$ is the Frobenius norm; $\sqrt{\mathcal{A}}$ stands for Hermitian square root of matrix $\mathcal{A}$; finally, capital (small) bold letters represent matrices (vectors).

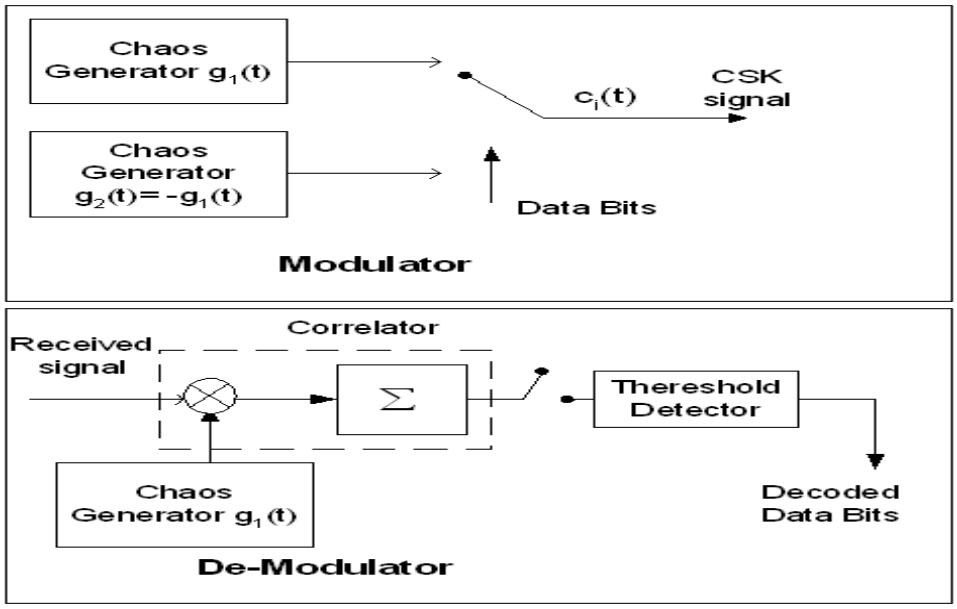

Figure 4.1: Modulator and demodulator block diagrams for chaos shift keying.

4.2 Chaos Shift Keying

As shown in chapter 3.2, the output of the CSK transmitter can be written as

$$c_k = \alpha_l g_{v,k} \tag{4.1}$$

The demodulation process for CSK is a simple coherent correlator at the receiver as shown in figure (4.1).

In this chapter, we use the simplest chaotic logistic maps for generation of chaotic sequences as in [17]

$$g_{n+1} = 1 - 2g_n^2 \tag{4.2}$$

which is the same as LCG1 in Chapter 3. Other LCGs can be used to improve the physical security performance. In this case, a simple LCG1 is used to minimize the complexity and study the use of chaos only in diversity technique.

4.3 OSTBC Encoding

At the output of CSK modulator, a series of N_s chip sequences are first converted into parallel streams before the OSTBC encoding process, each stream containing SF chip-symbols, where SF is the spreading factor in the CSK modulation function. In this paper we made the choice of N_s streams dependent on the OSTBC encoding matrix used. The OSTBC encoding of these streams of chip-symbols is done by taking one chip-symbol in each stream as the input symbol and then format these chips into a codeword matrix. Thus, the SF codeword matrices are constructed from these N_s input streams.

Denote the p^{th} output codeword matrix as $\mathbf{C}_p \in \mathbb{C}^{N_t \times N}$, which has N_t spatial dimensions and spans across N chip-symbol intervals. Since the number of baseband constellation points is finite, there is a limited number of possible OSTBC codeword matrices that can be generated; we denote this finite set as $\boldsymbol{\Upsilon}_p \ni \mathbf{C}_p$. Suppose that N_s input chip-symbols, which we collect into a row vector $\mathbf{s}_p = [c_{1,p}, \cdots, c_{m,p}, \cdots, c_{N_s,p}]$, are used to generate $\mathbf{C}_p$ by formatting $\mathbf{s}_p$ with an encoding matrix $\boldsymbol{\mathcal{G}}_p$ such that $\boldsymbol{\mathcal{G}}_p : \mathbf{s}_p \rightarrow \mathbf{C}_p$. According to [87], such encoding process can be mathematically expressed as

$$\mathbf{C}_p = \sum_{m=1}^{N_s} [c_{m,p}\mathbf{A}_m + c_{m,p}^{*}\mathbf{B}_m] \tag{4.3}$$

which are then split into a set of N_t parallel symbol sequences and transmitted during N chip intervals. The $\{\mathbf{A}_m, \mathbf{B}_m\}$ are matrices designed to satisfy the orthogonality condition that is well documented in both [87] and [88] as

$$\mathbf{C}_p\mathbf{C}_p^{*} = \sum_{m=1}^{N_s} \mid c_{m,p} \mid^2 \cdot \mathbf{I}_N, \tag{4.4}$$

where $(.)^*$ denotes the complex conjugate and $\mathbf{I}_N$ is an identity matrix of size N.

Since data symbols are ST block encoded in the proposed transmission structure, we regard all signal transmissions under consideration here as block transmissions. In the well-known STBC of [89], a different ST block encoding matrix requires different number of input chip symbols for different number of transmit antennas. The OSTBC encoding matrix $\boldsymbol{\mathcal{G}}4$ that we used for our system simulation is given by [89]

$$\boldsymbol{\mathcal{G}}4 = \begin{pmatrix} s_1 & s_2 & s_3 & s_4 \\ -s_2 & s_1 & -s_4 & s_3 \\ -s_3 & s_4 & s_1 & -s_2 \\ -s_4 & -s_3 & s_2 & s_1 \\ s_1^* & s_2^* & s_3^* & s_4^* \\ -s_2^* & s_1^* & -s_4^* & s_3^* \\ -s_3^* & s_4^* & s_1^* & -s_2^* \\ -s_4^* & -s_3^* & s_2^* & s_1^* \end{pmatrix} \tag{4.5}$$

which is employed for systems with $N_t = 4$.

4.4 Channel Model

Assume that the system operates in a typical cellular communication scenario where the base station (BS) antennas are placed at the building roof-top in an unobstructed environment and the mobile station (MS) is located at the street level surrounded by dense distribution of local scatterers. It is stated in [90]

that signal transmission in such an environment over a multipath channel leads to uncorrelated signal paths arriving at the MS but there would be partial correlation in the spatial domain at the BS. These propagation assumptions are normally used to model macrocell operation. Assume that a uniform linear array (ULA) configuration is used for N_t BS antennas with a spacing of d meters. The transmit spatial correlation matrix is defined in [91] as

$$\mathbf{R}_t = \frac{1}{L}\sum_{\ell=1}^{L} \mathbf{a}(\theta_\ell)\mathbf{a}^H(\theta_\ell), \tag{4.6}$$

where L denotes the number of dominant resolvable paths and

$$\mathbf{a}(\theta_\ell) := [1, e^{j\beta}, e^{j2\beta}, \cdots, e^{j(N_t-1)\beta}]^T$$

is the array propagation vector for the ℓ^{th} tap with an angle-of-arrival (AoA) of θ_ℓ impinging on the BS ULA. $\beta = [2\pi \cdot d \cdot \sin(\theta_\ell)]/\lambda$, λ being the carrier frequency wavelength. In general, $\mathbf{R_t}$ is an non negative-definite Hermitian Toeplitz matrix of the form

$$\mathbf{R}_t = [R_{uv}]_{N_t \times N_t} = \text{toeplitz}([1\ R_{12}\ R_{13}\ ...\ R_{1N_t}]), \tag{4.7}$$

where R_{uv} is the spatial correlation between signals from u^{th} and v^{th} antennas. Eigenvalue-decomposition (EVD) of $\mathbf{R}_t$ can be expressed as $\mathbf{V}\mathbf{R}_t\mathbf{V}^H = \mathbf{\Lambda}$, where $\mathbf{V} = [\boldsymbol{\upsilon}_1, \cdots, \boldsymbol{\upsilon}_{N_t}]$ is a unitary matrix with columns that are the eigenvectors and $\mathbf{\Lambda} = \text{diag}[\omega_1, \cdots, \omega_n, \cdots, \omega_{N_t}]$ is a diagonal matrix contains the corresponding eigenvalues.

We consider multi-input multi-output (MIMO) frequency-selective channel between the transmitting and receiving antennas. Following [92], this under-

lying frequency-selective channel can be modelled as a tapped delay line that represents an L^{th}-order finite-impulse response (FIR) filter whose coefficients are τ-samples of the impulse response $\{h_{i,j}(\tau;t)\}$ of the channel corresponding to the $(i,j)^{\text{th}}$ receive-transmit antenna pair

$$h_{i,j}(\tau;t) = \sum_{\ell=1}^{L} \alpha_{i,j}(\ell;t)\delta(\tau - n_\ell), \tag{4.8}$$

where t represents time, τ is the time-delay, $\alpha_{i,j}(\ell;t)$ is the ℓ^{th} path complex fading coefficient, $\delta(\cdot)$ is the Dirac delta function, and $n_\ell = \ell/W$ is the delay of the ℓ^{th} path. Thus, the channel impulse response includes the channel fading effect and the relative delay spread of the multi-paths. Denote the discrete-time baseband equivalent impulse response vector as $\mathbf{h}_{i,j}[n] = [\alpha_{i,j}(1;nT), \cdots, \alpha_{i,j}(L;nT)]$ for the n^{th} chip interval, where T is the total time duration of one OSTBC codeword. In this paper, $\{\alpha_{i,j}(\ell;nT)\}$ are modelled as correlated circularly symmetric complex Gaussian random variables with zero mean.

Let us denote the correlated MIMO channel impulse response matrix for the p^{th} OSTBC codeword block as $\mathbf{H}[n;p] \in \mathbb{C}^{N_r \times N_t}$. The $(i,j)^{\text{th}}$ element, which represents the subchannel gain between the i^{th} receive antenna and the j^{th} transmit antenna, is defined as

$$h_{i,j}[n;p] := \sum_{\ell=1}^{L} \alpha_{i,j}(\ell;nT). \tag{4.9}$$

According to [90], we can also express the channel matrix as $\mathbf{H}[n;p] = \overline{\mathbf{H}}[n;p]\sqrt{\mathbf{R}_t}$, where $\overline{\mathbf{H}}[n;p]$ can be thought of as a *pre-whitened* channel matrix with independent circularly symmetric complex Gaussian random variables from $\mathcal{CN}(0,\sigma_h^2)$.

Furthermore, quasi-static fading is assumed throughout the duration of one STBC codeword length (i.e., if N is the length of the p^{th} codeword, then $\mathbf{H}[1;p] = \mathbf{H}[n;p]\,|n = 1, \cdots, N)$, but fading may vary from one block to another. Therefore, the timing index n will be dropped and $\mathbf{H}[n;p]$ will hereafter be written as $\mathbf{H}_p$.

4.5 Adaptive Eigen Beamforming

In enhancing the received signal-to-noise ratio (SNR) and thus the probability for correct detections of transmitted OSTBC codeword, signal transmission in the eigen-modes of the correlation matrix, eigen weight mapping is performed across the space dimension of the OSTBC codeword $\mathbf{C}_p$ prior to transmission as in [86]. Mathematically, it can be expressed as $\mathbf{W}^H\mathbf{C}_p$, where $\mathbf{W} = [\mathbf{w}_1, \cdots, \mathbf{w}_{N_t}]$ is the eigen weight mapping matrix and $\mathbf{w}_j = \boldsymbol{\upsilon}_j$. Then signal transmission on different eigenvectors of $\mathbf{R}_t$ amounts for transmitting N_t orthonormal beams in the direction of the dominant multipaths seen by the transmitter.

4.6 System Simulation

The system diagram in figure (4.2) showed the proposed transceiver structure with CSL modulator, OSTBC encoder, and eigen weight mapper at the transmitter. The transmitted signal is corrupted by frequency selective rayleigh fading (for microcell wireless channel) before arriving at the receiver.

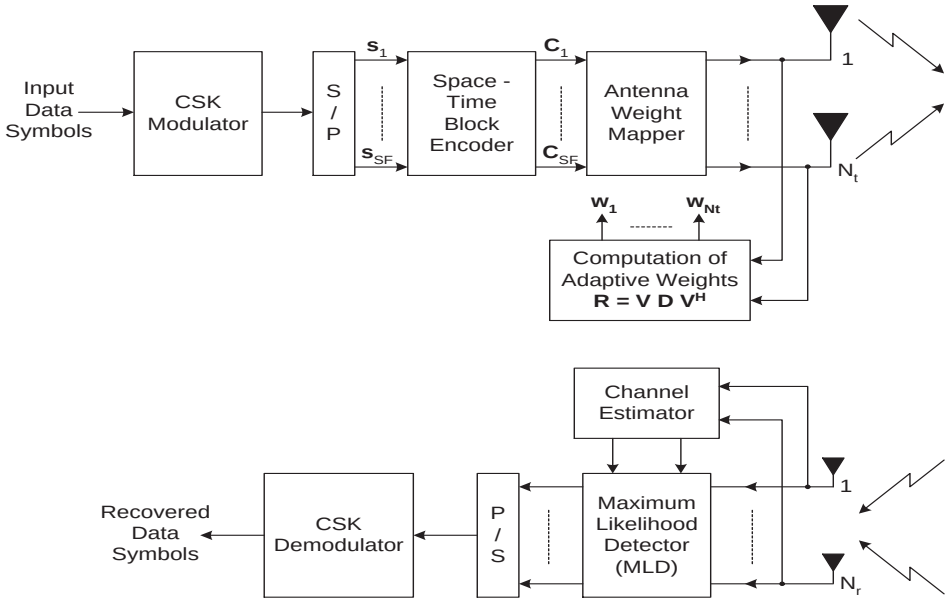

Figure 4.2: General structure of the proposed system structure.

At the receiver, OSTBC codeword signals are received from N_r antennas. The discrete time baseband equivalent expression of the received signal has the form

$$\mathbf{Y}_p = \overline{\mathbf{H}}_p \sqrt{\mathbf{R}_t} \mathbf{W}^H \mathbf{C}_p + \mathbf{E}_p \ , \tag{4.10}$$

where $\mathbf{E}_p$ is the receiver noise matrix and its elements are modelled as uncorrelated white Gaussian random variables taken from $\mathcal{N}(0, \sigma_n^2)$.

In order to perform OSTBC codeword decoding, channel estimation is needed to be performed first by correlating the embedded pilot symbols sent with the data signal with a prior known sequence. The estimation results from N_r receive antennas are then fed into the maximum likelihood decoder (MLD) for the OSTBC codeword decoding. The general decision matrix for the evaluation

of transmitted data can be written as

$$\widehat{\mathbf{C}}_p = \arg \min_{\mathbf{C}_p \in \mathbf{\Upsilon}_p} \|\mathbf{Y}_p - \overline{\mathbf{H}}_p \sqrt{\mathbf{R}_t} \mathbf{W}^H \mathbf{C}_p\|_F^2 \ . \tag{4.11}$$

A more specific decoding algorithms can be found in [89] for various sizes of OSTBC encoding matrices. The final state to recover the original bit stream signal is only a simple parallel to series conversion on the $\widehat{\mathbf{C}}_p$ then passed thought a CSK demodulator (simple correlator) as described in Section 4.2.

In order to simulate the proposed transmission structure in frequency-selective Rayleigh fading channels, the following parameters and simulation assumption were adopted: BPSK baseband modulation is used, the spatial channel correlation is modelled using the Macrocell GBHDS channel model in [12], $\mathcal{G}_4$ encoding matrix in [88] is utilized for OSTBC codeword construction, and hence $Nt = 4$, $N_r = 2$ were employed.

Figures. (4.3 - 4.5) show the BER performance of CSK with eigen-beamforming and OSTBC for different spreading factors. As expected, combining eigen-Beamforming with OSTBC in CSK will outperform those systems without any diversity technique, or systems with only OSTBC. Generally, at low Eb/No, the performance gain is more dependent on the coding gain of OSTBC, else at higher Eb/No, the gain is more dependent on the diversity gain. Comparing the BER ranges in figures (4.3 - 4.5), we can see that an increase in the spreading factor will lead to a better BER performance. However, figure (4.6) does show that there is a convergence point where increasing SF will not provide much different performance gain. Hence, choosing the SF should be carefully considered, keeping in mind that increasing SF will increase the processing time. The optimum value in this case is around $SF = 100$.

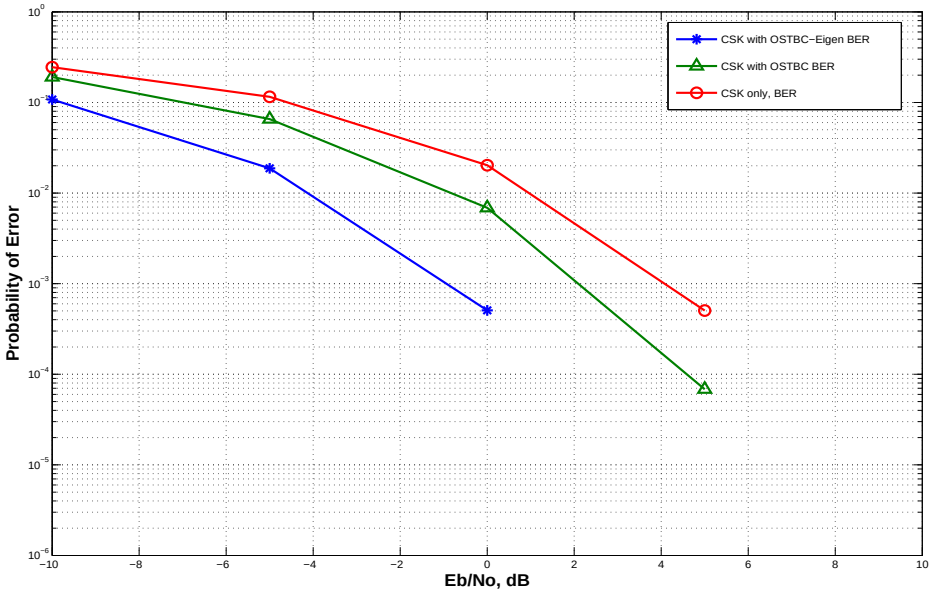

Figure 4.3: BER vs Eb/No performance for CSK with eigen-beamforming and OSTBC, Nr=1, 4-tap correlation, and $SF = 16$.

4.7 Conclusions

A secure communication with diversity technique is proposed in this chapter. The use of a chaotic generator for spreading can provide a more secure communication than using the conventional digital spreading. The scheme is combined with space-time coding and eigenbeamforming, giving a much lower bit error rate and hence, increased security. The proposed scheme can be used in wireless communication systems where security is the concern. To enhance the security performance, a larger spreading factor can be used, but it is shown that there is a threshold for this increase, after which no BER performance advantage can be obtained.

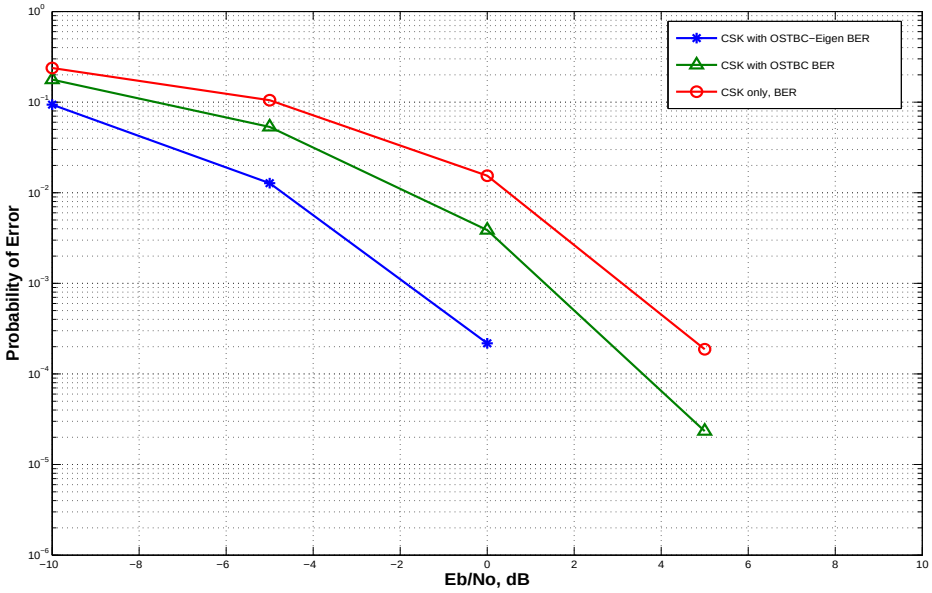

Figure 4.4: BER vs Eb/No performance for CSK with eigen-beamforming and OSTBC, Nr=1, 4-tap correlation, and $SF = 32$

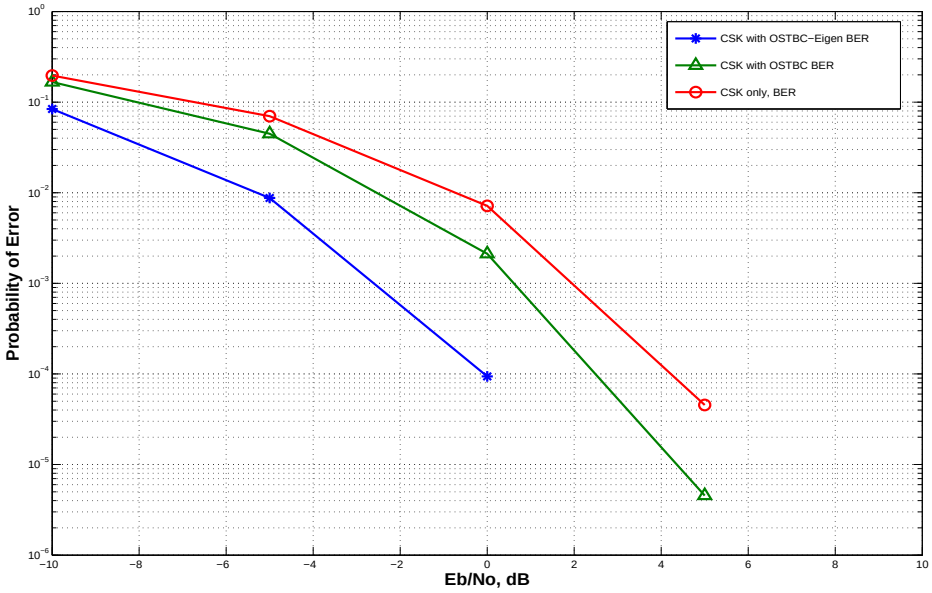

Figure 4.5: BER vs Eb/No performance for CSK with eigen-beamforming and OSTBC, Nr=1, 4-tap correlation, and $SF = 64$

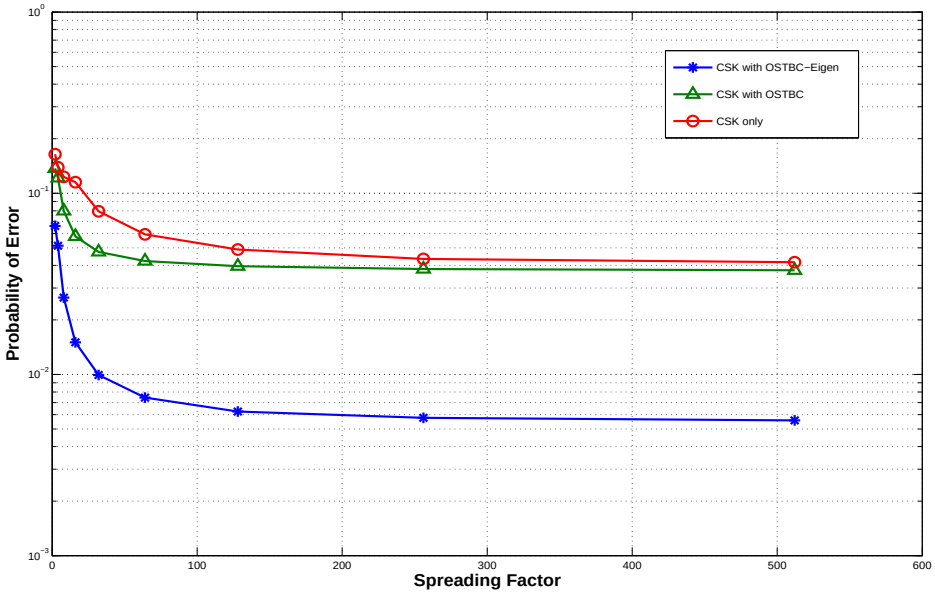

Figure 4.6: BER vs SF performance for CSK with eigen-beamforming and OSTBC, Nr=1, 4-tap correlation, and Eb/No = -5 dB.

Chapter 5

Chaos in Multi-Carrier Communications

5.1 Introduction

In the previous two chapters, we had looked at the application of chaos theory in digital communications. We particularly considered chaos shift keying (CSK) to transmit a single bit information in wireless environment. However, Multi-carrier Modulation (MCM) has become a key communication system technology. In this chapter, we study the possible use/or combination of chaos theory in MCM scheme.

The fundamental idea of MCM transmission is to transmit different signals in parallel on different frequencies or channels. The conventional method using FFT/IFFT operation for the MCM, also referred to as orthogonal frequency division multiplexing (OFDM), is proposed by Weinstein and Ebert in 1971 [93]. In the past decade, due to the enormous progress and advance in signal processing, these ideas have been put in practical use for both wire and wireless communication such as: digital video broadcasting (DVB), digital subscriber line (DSL), digital audio broadcasting (DAB), power line communications (PLC),

wireless LAN (802.11), and European HIPPERLAN/2. However, OFDM suffers from few drawbacks that are related to peak-to average power ratio (PAPR) and bandwidth efficiency. These drawbacks have drawn the attention to use other means of modulation for the OFDM. Hence, wavelet-based OFDM gained its popularity in literature, thus it has been proposed for practical use in wireless LAN 802.16 [94].

Wavelet-OFDM also sometimes referred to as fractal modulation was proposed in early 90's by Wornell and Oppenheim [95, 96]. The signals can carry information distributed over multiple time scales and frequency bands just like the OFDM do. The difference is that OFDM does have a uniform distribution whereas WOFDM is multirate - distributed depending on the mother wavelet. The multirate diversity ability of WOFDM offers several advantages to mobile communications as compared to OFDM. Wavelet-OFDM (WOFDM) can provide less overhead to the physical link because it does not require a cyclic prefix, unlike the traditional OFDM [94, 97]. Wavelet-OFDM also provides better combat to narrowband interference and inter-channel interference (ICI) as compared to the conventional OFDM, where WOFDM does not need cyclic prefix due to its high spectral containment between subchannels.

On the other hand, the Forth Generation (4G) mobile communications is particular interested in a combination of CDMA and OFDM. This will enable high data rates and high user capacities due to the inherent error resistance in a multi-path environment for both CDMA and OFDM systems. As a result, there is generally an increasing interest in studying the combination of OFDM and CDMA (OFDM-CDMA) [98, 99, 100], which is sometimes also referred to as multi-carrier CDMA (MC-CDMA). OFDM-CDMA can provide frequency diversity in a frequency selective channel because individual data symbols are

spread over the entire bandwidth using spreading code in the frequency domain [98, 99]. In contrast, the CDMA code can be generated using a chaos generator. Chaotic sequences generated from the chaotic generator have been proven to provide performance close to the ideal case [19, 21, 101]. In this chapter,we provide a comprehensive study for the combination of the chaos spread spectrum with MCM schemes, namely, Chaos shift keying-Orthogonal frequency division multiplexing (CSK-OFDM) and Chaos shift keying-Wavelet based orthogonal frequency division multiplexing (CSK-WOFDM). We will also study the chaos-based CDMA and PN-based CDMA in the multi-user environment and their use in conjunction with OFDM.

5.2 CSK-OFDM and CSK-WOFDM

CSK modulation and demodulation is as shown in Chapters 3 and 4. Figure (5.1) shows a block diagram of the the simulated CSK-OFDM system. In CSK-OFDM system, the received OFDM symbol is formulated as follows:

$$y_n = \text{IFFT}(s_n)h_n + \eta_n \tag{5.1}$$

where η_n represents uncorrelated additive white Gaussian noise, h_n is the communication channel impulse response modelled using Rayleigh fading, $s_n = d_t c_t[m]$ is the transmitted CSK symbol in the n^{th} carrier duration of a single OFDM symbol, d_t is data bits, and $c_t[m]$ is t^{th} CSK squence with m as a spreading factor. For simplicity, the channel impulse response is assumed to be known to the receiver. Therefore, the received CSK signal after OFDM demodulation

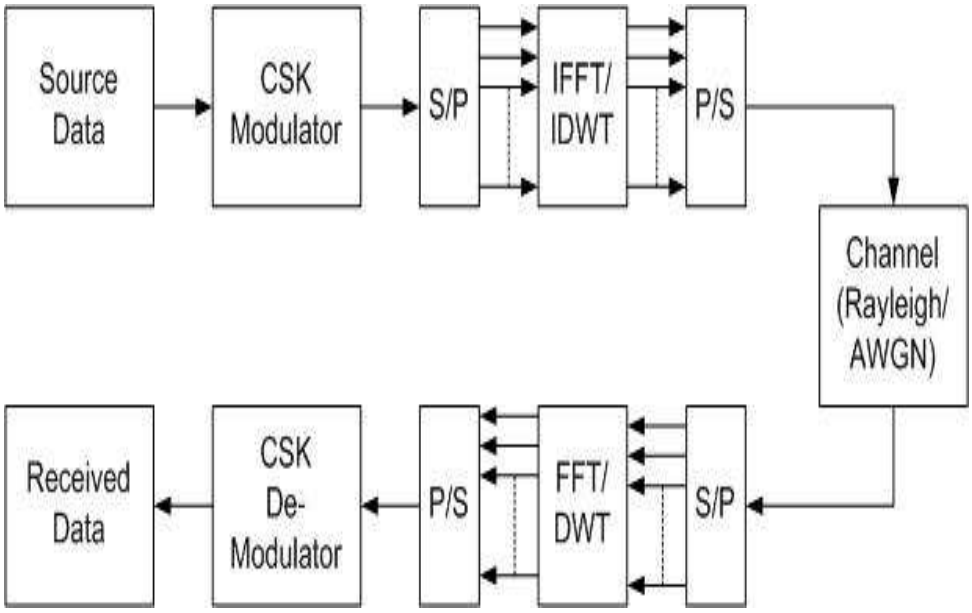

Figure 5.1: A block diagram for the simulated CSK-OFDM and CSK-WOFDM systems.

is assumed to have perfect channel estimation $r_t = \mathrm{FFT}(y_n h_n^*)$.

As for wavelet-based OFDM, the IFFT and FFT blocks are simply replaced by an inverse discrete wavelet transform (IDWT) and discrete wavelet transform (DWT) for simulation. The wavelet transform is a generalized Fourier transform operation that allows different dilations and shifts that provide certain specific properties. In this simulation we consider Haar wavelet due to its simplicity. Moreover, Haar wavelet is a discontinuous function that will have no Gibb's phenomenon [102], hence it will help to reduce the PAPR problem. The representation for Haar wavelet is [102]:

$$\Psi(t) = \begin{cases} -1 & \text{, for } 0 \leq t < 1/2 \\ 1 & \text{, for } 1/2 \leq t < 1 \\ 0 & \text{, otherwise} \end{cases} \tag{5.2}$$

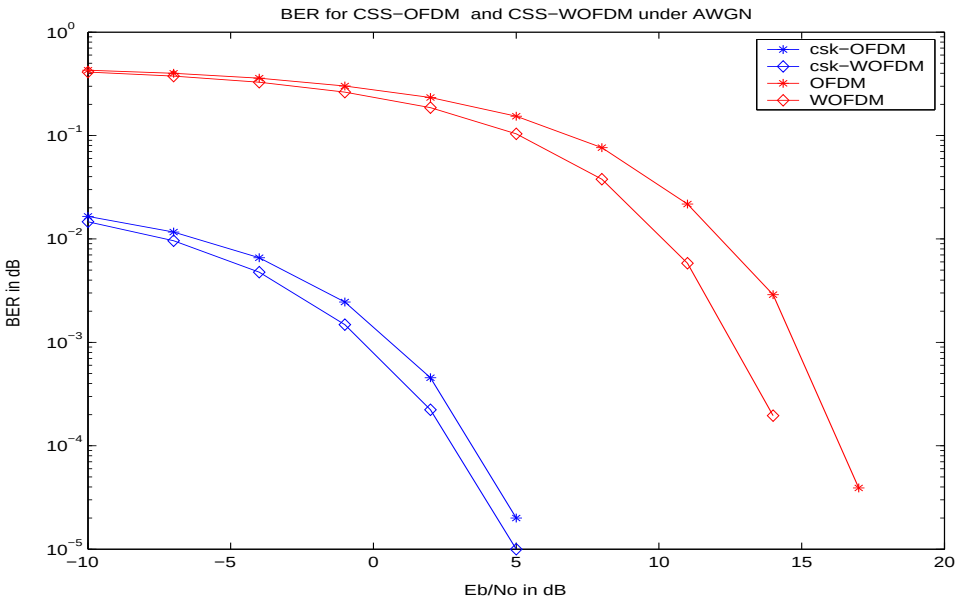

Figure 5.2: BER performance of OFDM, WOFDM, CSK-OFDM and CSK-WOFDM systems in AWGN environment.

Figure (5.2) shows the BER performance for the OFDM, WOFDM, CSK-OFDM and CSK-WOFDM systems in AWGN channel. Figure (5.2) shows that wavelet-based OFDM provides better BER performance than the FFT-based OFDM. When a spreading system is used in conjunction with OFDM, the CSK-OFDM and CSK-WOFDM provided better BER performance.

Figure (5.3) shows the BER performance for the OFDM, WOFDM, CSK-OFDM and CSK-WOFDM systems in a Rayleigh fading channel with AWGN environment. Figure (5.3) provides a conclusion similar to that of figure (5.2) that WOFDM generally provides better BER performance. Both CSK-OFDM and CSK-WOFDM provide a huge gain in the BER performance under Rayleigh fading environment. Hence, the combination of spread spectrum with MCM will provide robustness for wireless communications.

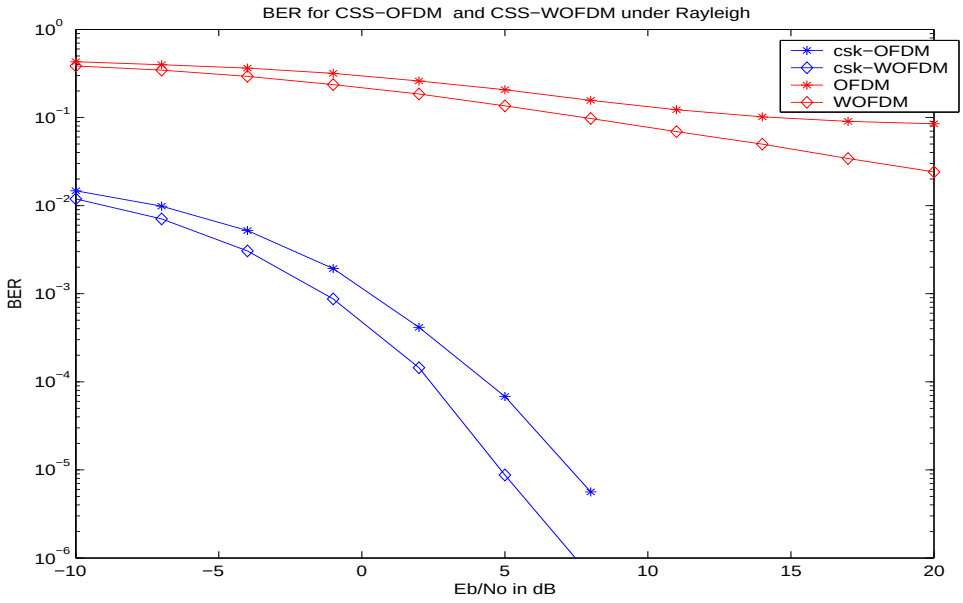

Figure 5.3: BER performance of OFDM, WOFDM, CSK-OFDM and CSK-WOFDM systems in Rayleigh environment

5.2.1 Discussion

We presented a combination of chaos shift keying with MCM for both OFDM and WOFDM systems. The use of CSK can increase the security prospective of the system due to it bifurcation behavior when varying the initial condition. On the other hand, wavelet-based OFDM is shown to provide better BER performance as well as lower PAPR. Simulation showed that the average PAPR for CSK-OFDM is nearly at 4 but for CSK-WOFDM the average PAPR is only at 2. Hence, there would be an increase in the system power efficiency and performance if wavelet-based OFDM is used.

5.3 Chaos CDMA

We used the following Logistic Chaos Generator 1 (LCG1) in Chapter 3 to generate chaotic sequences for Chaos CDMA:

$$x_{n+1} = 1 - ax_n^2. \tag{5.3}$$

Other LCGs can also be used and, as shown in Chapter 3, the performance may vary depending on thr chaos generator, however, the variation is minimum. Hence, a simple LCG1 is used to minimize the complexity and study the use of chaos in multi-carrier communications.

This system was studied in [17, 18, 19] for CDMA systems. The resulting chaotic sequences will always converge inside the open interval $(-1, 1)$ under the conditions that the initial value $x_o = x(0)$ lies in the interval $(-1, 1)$, and $a = 2$ to allow the system to become a non-linear dynamic system varying within the interval $(-1, 1)$. In CDMA systems, the spreading sequences are usually in binary format. Hence, a quantization function $Q(x)$

$$Q(x) = \begin{cases} 1 & \text{, if } x > 0 \\ -1 & \text{, otherwise} \end{cases} \tag{5.4}$$

is used to convert the recursive chaotic sequences into binary chaotic sequences.

Figure 5.4 (above) shows the auto-correlation function of two chaotic sequences generated by (5.3) with two initial values $x(0) = 0.07$ and $x(0) =$

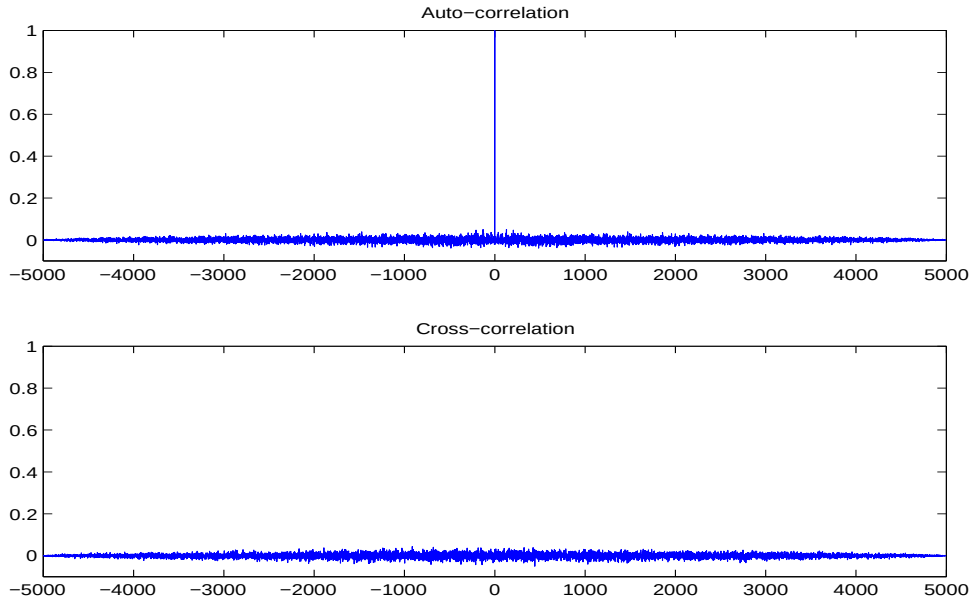

Figure 5.4: Above: auto-correlation function of two chaotic sequences generated by (5.3) with two initial values $x(0) = 0.07$ and $x(0) = 0.07001$. Below: cross-correlation of the above two chaotic sequences.

0.07001; it is evident that these correlation properties are similar to those of random white noise even. Figure 5.4 (below) shows the cross-correlation of the above two chaotic sequences, which is nearly zero everywhere, indicating that the two sequences are uncorrelated, despite the fact that their initial values are just slightly different. This mean that, the generation of binary chaotic sequences is very sensitive to the initial condition (value). A slight difference in the initial condition will generate a totally different chaotic sequence.

5.3.1 Chaos CDMA Simulation and Results

We consider a simple BPSK communication system as shown in figure (5.5).

The received signal before CDMA demodulation for a single user can be

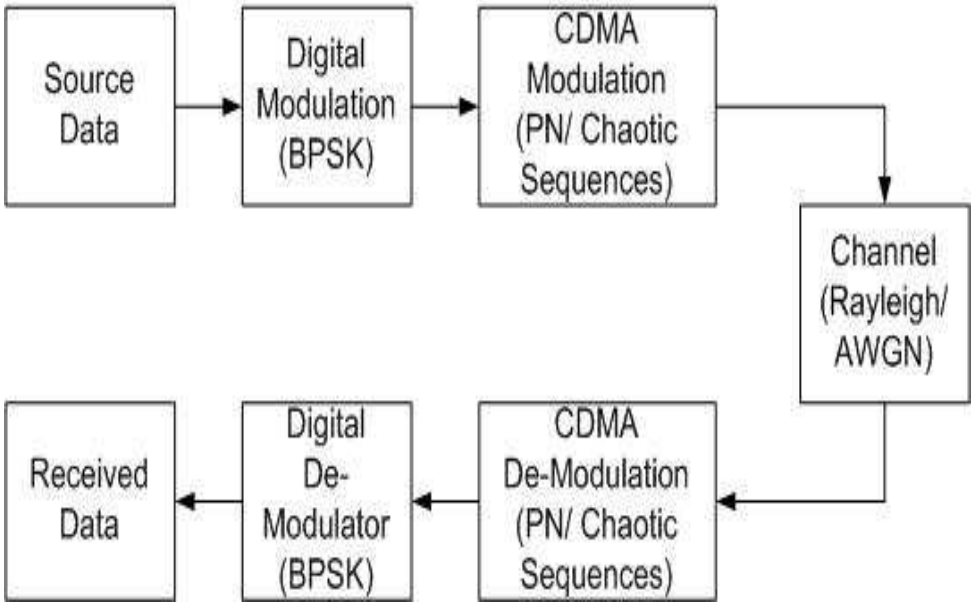

Figure 5.5: A block diagram for the simulated CDMA system.

formulated as:

$$r_k = s_k h_k + \eta_k \tag{5.5}$$

where η_k is additive Gaussian noise, h_k is the communication channel impulse response modelled as Rayleigh fading, and s_k is the k^{th} transmitted symbol formulated as

$$s_k = \alpha_k c_l \tag{5.6}$$

where $l = 2\beta(k-1)+1, 2\beta(k-1)+2, ..., 2\beta k$. The factor 2β is defined as the spreading factor, α_k is the BPSK symbol to be sent during the k^{th} bit period, and c_l is the binary CDMA spreading sequence code.

The received signal before CDMA demodulation for multiple users can be formulated as:

$$r_k = \sum_{m=1}^{M} s_{(k,m)} h_k + \eta_k \tag{5.7}$$

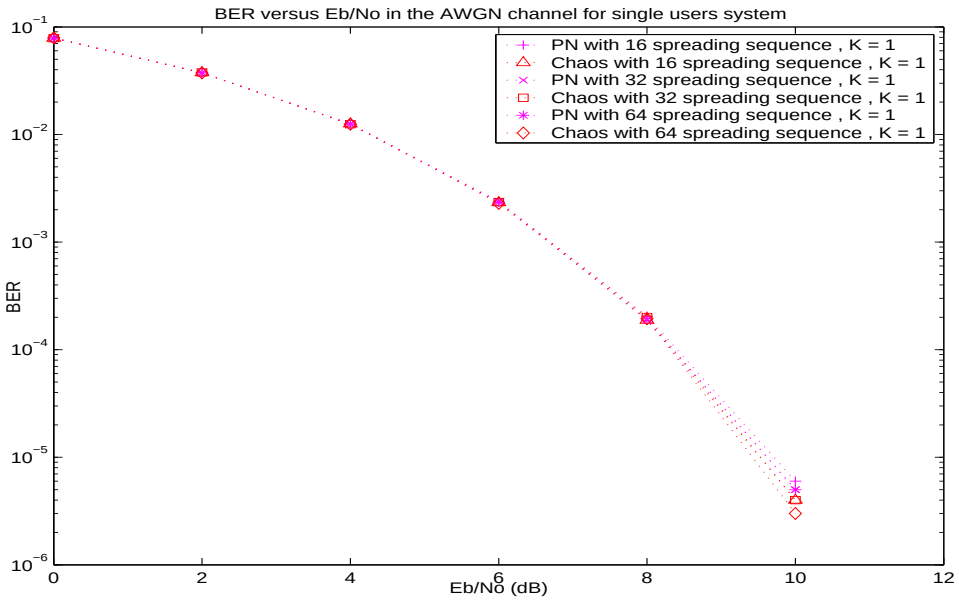

Figure 5.6: BER performance of the chaos-based CDMA and the PN-based CDMA in AWGN in a single-user environment with sequence lengths 16, 32 and 64.

M being the total number of users.

Additive White Gaussian Noise Channel

Additive white Gaussian noise (AWGN) channel is one of the simplest channel models, which is widely used for modelling wired systems.

Figure (5.6) shows the BER performance for the uncoded chaos-based CDMA and the uncoded PN-based CDMA systems in AWGN channel condition with a single-user environment. It is evident that both systems provide similar performance in a single-user environment.

Figures (5.7, 5.8 and 5.9) show the BER performance for the uncoded chaos-based CDMA and the uncoded PN-based CDMA under the AWGN channel condition for multi-user environment. It is evident that chaotic sequences provide better BER performance than PN sequences in multi-user environment.

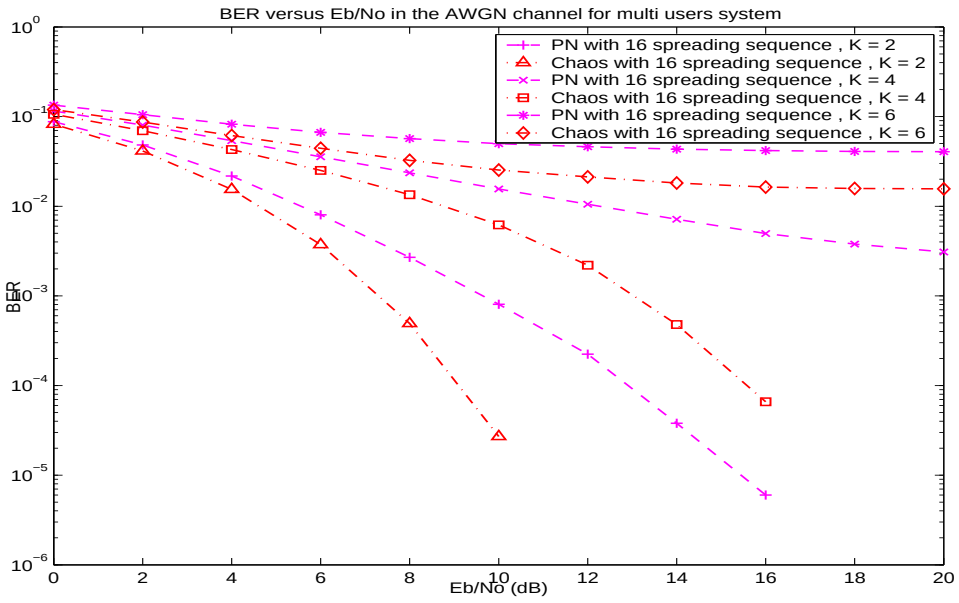

Figure 5.7: BER performance of the chaos-based CDMA and the PN-based CDMA in AWGN in multi-user environment with sequence length 16.

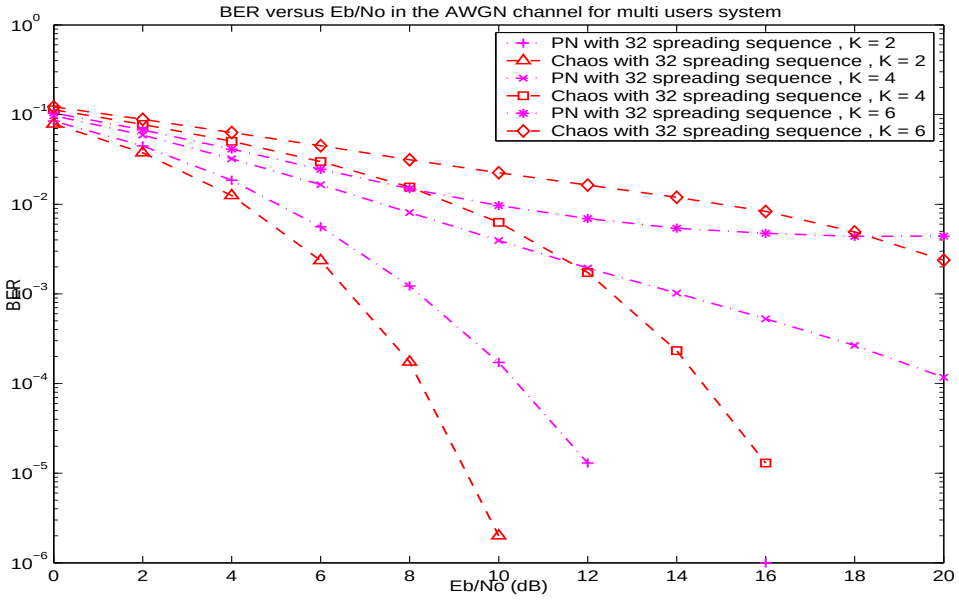

Figure 5.8: BER performance of the chaos-based CDMA and the PN-based CDMA in AWGN in multi-user environment with sequence length 32.

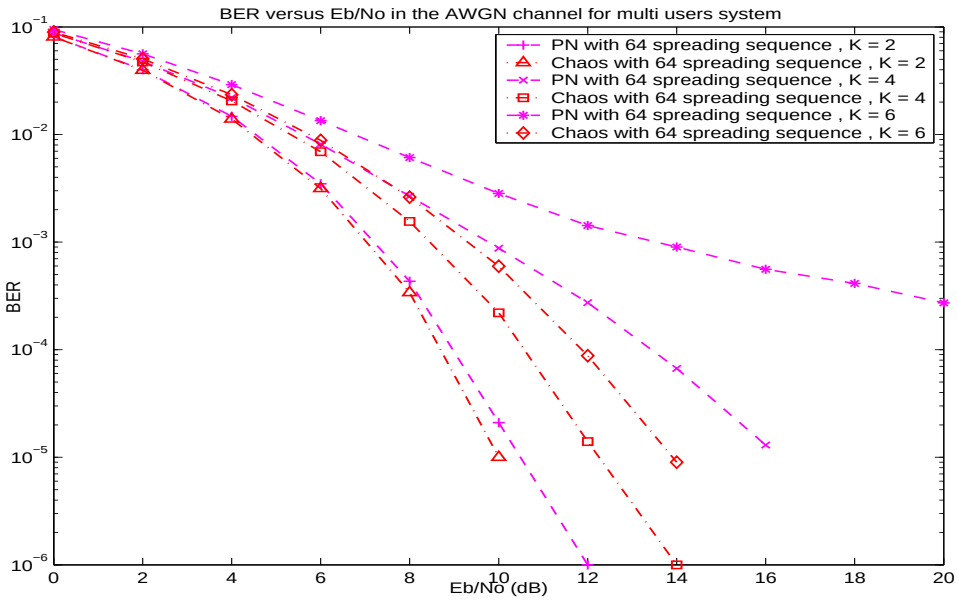

Figure 5.9: BER performance of the chaos-based CDMA and the PN-based CDMA in AWGN in multi-user environment with sequence length 64.

Rayleigh Fading Channel

Rayleigh fading channel is the most commonly used channel for wireless communications. Rayleigh fading channel can be modelled in the equivalent complex baseband described by a zero-mean complex Gaussian random process

$$\mu(t) = \mu_1(t) + j\mu_2(t) \tag{5.8}$$

$\mu_1(t)$ and $\mu_2(t)$ are statistically uncorrelated and assumed that it is the real-valued Guassian random process. In this simulation, we assume that the receiver and the transmitter are in stationary condition (flat fading), hence Doppler shift is not applied.

Figure (5.10) shows the BER performance for the uncoded chaos-based CDMA and the uncoded PN-based CDMA in the Rayleigh fading channel with

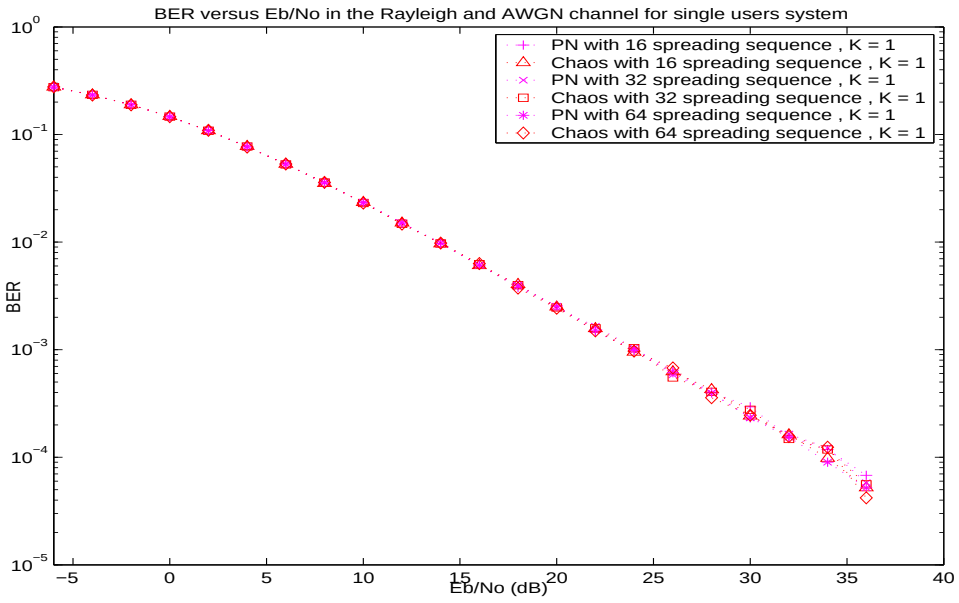

Figure 5.10: BER performance of the chaos-based CDMA and the PN-based CDMA in Rayleigh channel in single-user environment with sequence length 16, 32, and 64.

AWGN in single-user environment. It is shown that both systems provide similar performance.

Comparing the wired communication systems (with channel modelled as AWGN channel) to wireless communication systems (with Rayleigh fading channel), wireless systems performed worse than wired systems.

Figures (5.11, 5.12 and 5.13) show the BER performance for the uncoded chaos-based CDMA and the uncoded PN-based CDMA in Rayleigh fading channel with AWGN in multi-user environment. In general, chaotic sequences provide better BER performance than PN sequences, especially in short sequence length. Note that when sequence length is equal to 64, both PN and chaotic sequences provide similar results, hence, more users can be added to increase the system capacity.

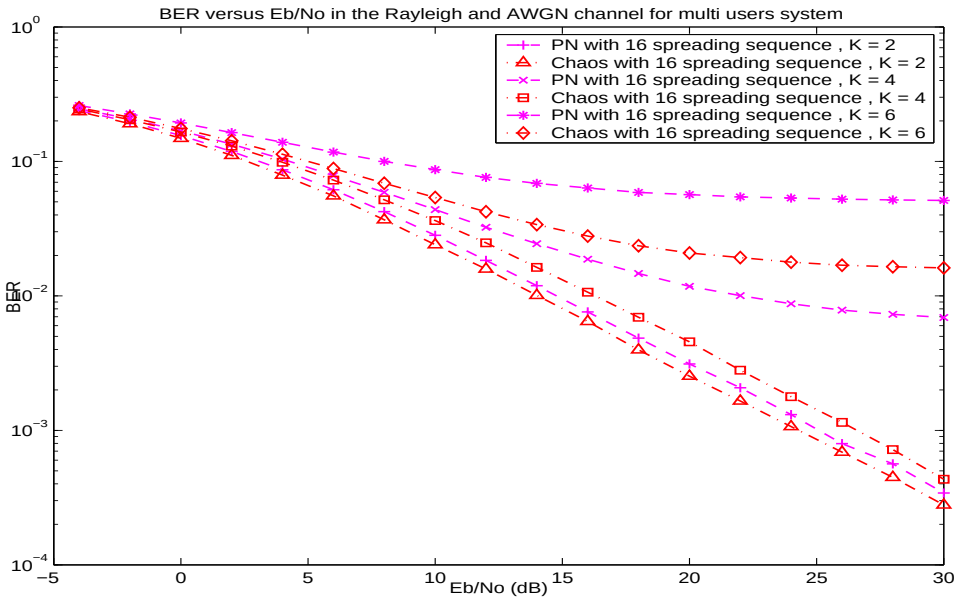

Figure 5.11: BER performance of the chaos-based CDMA and the PN-based CDMA with Rayleigh channel in multi-user environment using a sequence length of 16.

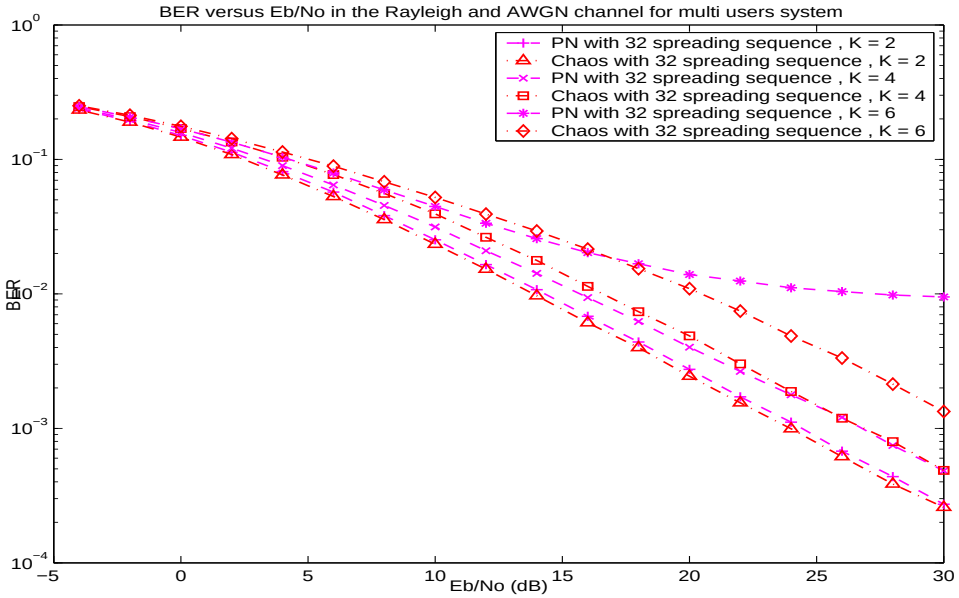

Figure 5.12: BER performance of the chaos-based CDMA and the PN-based CDMA with Rayleigh channel in multi-user environment using a sequence length of 32.

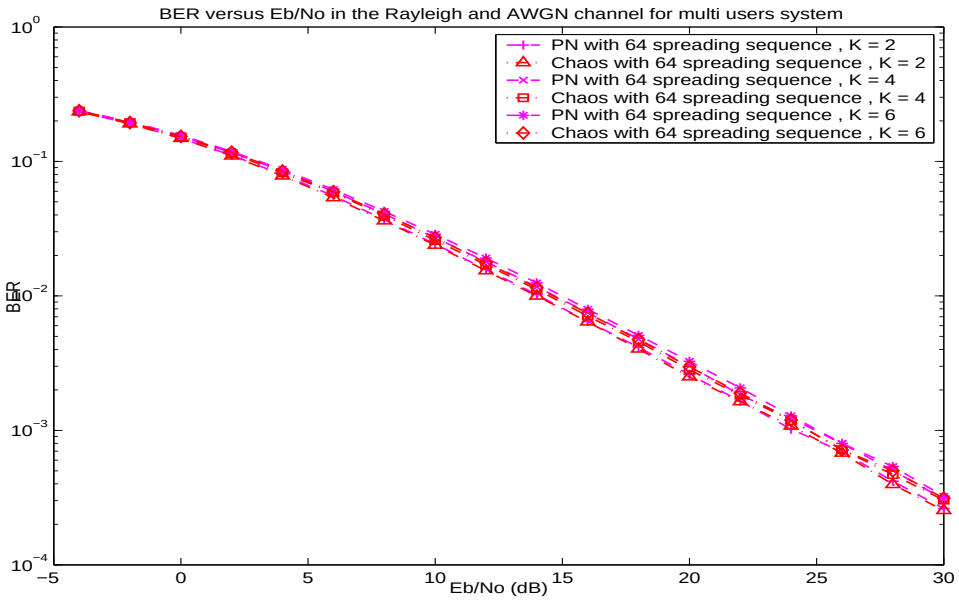

Figure 5.13: BER performance of the chaos-based CDMA and the PN-based CDMA with Rayleigh channel in multi-user environment using a sequence length of 64.

5.3.2 Discussion

We presented a comparative study between a simple recursive chaotic sequence and a PN sequence for CDMA communication systems. Chaotic sequences provide noise-like features, with auto-correlations and cross-correlations similar to white noise processes. Theoretically, the chaotic sequences are unlimited in length, hence suitable for large number of users. Due to its bifurcation behaviors, chaotic sequences can be useful for secure communications. It is very hard to predict a chaotic pattern even if the generating chaotic function is known to the interceptor. Generally, under static stationary condition, Doppler effect is not considered in this study. Doppler spread degrades the performance of communication systems but not individual signals, hence it was not taken into consideration when comparing the performance between PN and chaos sequences.

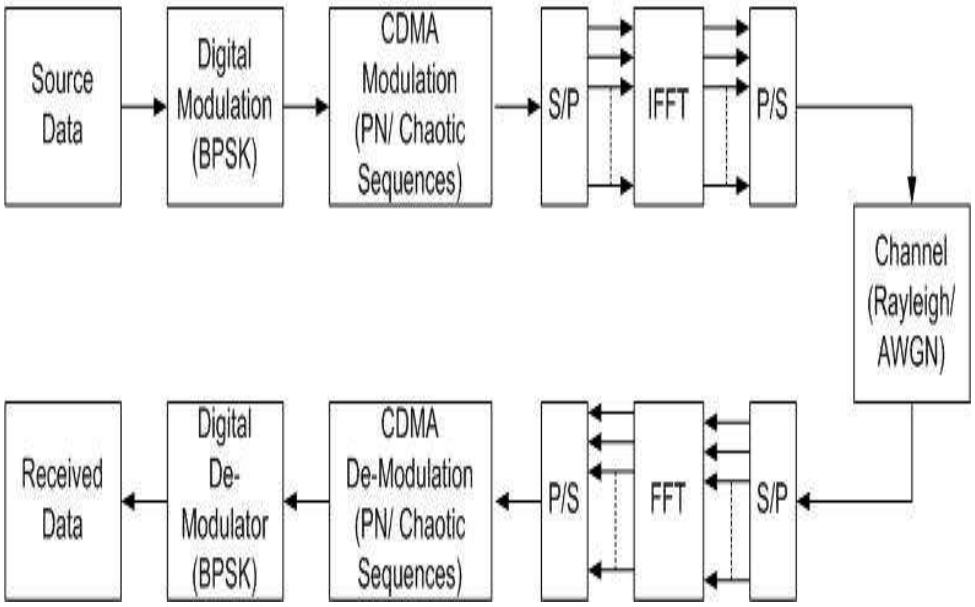

Figure 5.14: A block diagram for the simulated CDMA-OFDM system.

Under both AWGN and rayleigh fading channels, chaos-based CDMA do provide little improvement due to the unrepeated, uncorrelated, and non-linear properties of chaos signals. These can be seen in figure(5.7 5.8, 5.9,5.11,5.12).

5.4 Chaos CDMA-OFDM

The simple block diagram of the Chaos-based and PN-based CDMA-OFDM is shown in figure (5.14).

The received OFDM symbol before OFDM demodulation can be formulated as:

$$y_n = \text{IFFT}(s_n)h_n + \eta_n \tag{5.9}$$

where η_n represents an uncorrelated additive white Gaussian noise, h_n is the communication channel impulse response, and $s_n = \sqrt{P_t}d_t c_t[m]$ is the trans-

mitted CDMA symbol in n^{th} carrier duration of a single OFDM symbol. P_t is the transmit signal power, d_t is BPSK signal, and $c_t[m]$ is t^{th} CDMA spreading code with m as a spreading factor. Note that in this simulation, three different system conditions are considered. The first condition is $m = n$, i.e., the spreading factor is equal to the number of OFDM carriers (1 CDMA symbol to 1 OFDM symbol ratio). The OFDM-CDMA system will have the same transmission rate as that of the CDMA system. The second condition is $2m = n$; where the spreading factor is now smaller than the number of OFDM carriers (a ratio of 2 CDMA symbols to 1 OFDM symbol). The OFDM-CDMA system will have higher transmission rate than the CDMA system. The third condition is $m = 2n$; where the spreading factor is larger than the number of OFDM carriers (a ratio of 1 CDMA symbol to 2 OFDM symbol). The OFDM-CDMA system will have slower transmission rate than the CDMA system. However this should provide a better BER performance, as the following results will show.

All simulations run for 100 realizations. Hadamard Code sequences are used to represent PN CDMA code sequences. Since there are limited number of Hadamard codes, the codes will be reused when this number is exceeded. As a result, the reuse of the code is decreasing the security of the system, since the attacker can easily predict the code. On the other hand, the generation of binary chaotic code follows the description in section above. We will consider two important channel models to verify our claims.

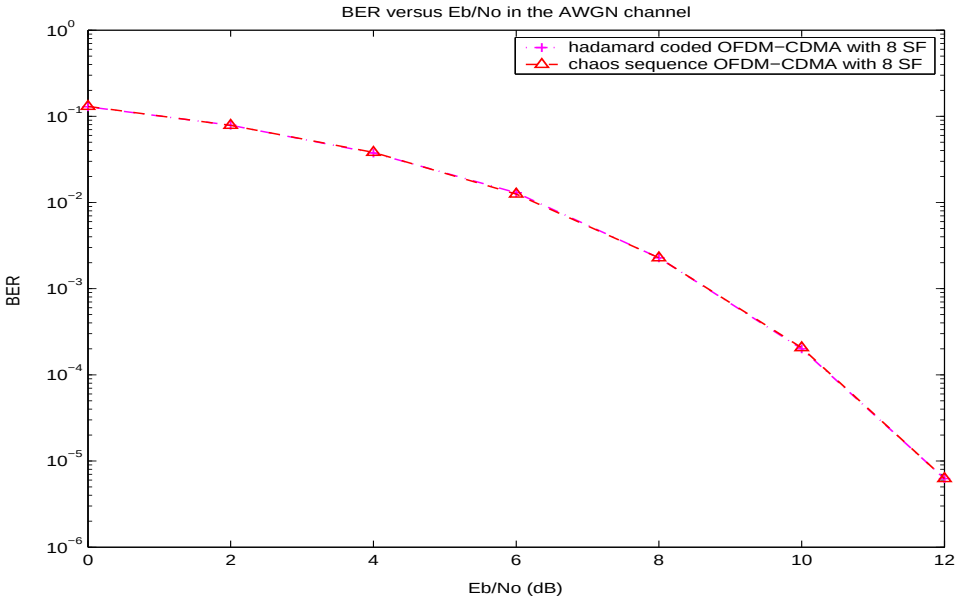

Figure 5.15: BER performance for the chaos-based and the PN-based OFDM-CDMA in AWGN (SF=8, FFT size = 16).

5.4.1 Additive White Gaussian Noise

The received signal after OFDM demodulation is:

$$r_n = \text{FFT}(\text{IFFT}(s_n) + \eta_n) \tag{5.10}$$

$$= \text{FFT}(\text{IFFT}(s_n)) + \hat{\eta_n} \tag{5.11}$$

The term $\hat{\eta_n} = \text{FFT}(\eta_n)$ represents uncorrelated Gaussian noise.

Figures (5.15, 5.16 and 5.17) show the BER performance for the uncoded chaos-based OFDM-CDMA and the uncoded PN-based OFDM-CDMA in the AWGN channel. In general, both systems provide similar BER performance. It is also shown that a larger spreading factor will provide a better BER performance, however in doing so, it will reduce the system capacity.

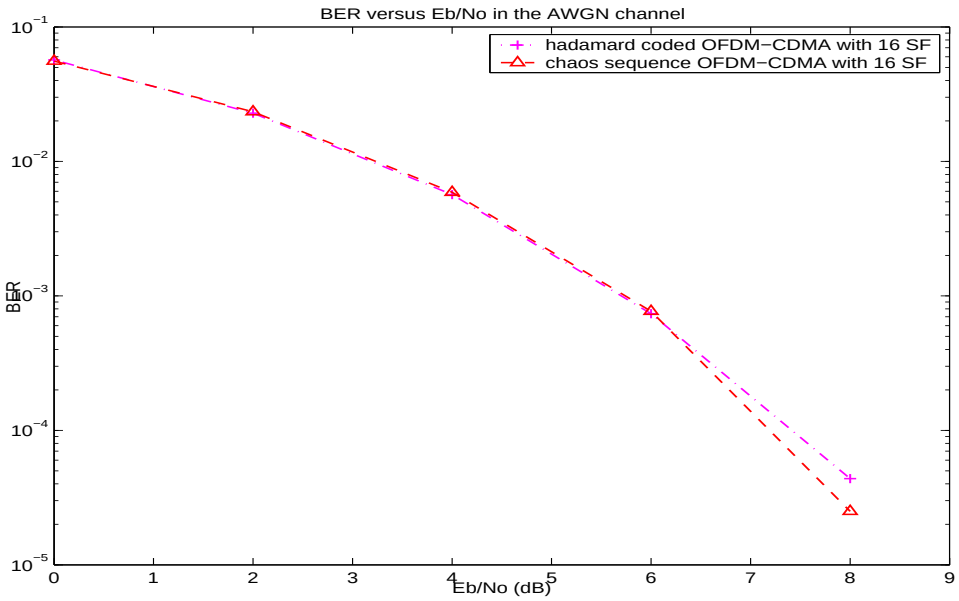

Figure 5.16: BER performance for the chaos-based and the PN-based OFDM-CDMA in AWGN (SF=16, FFT size = 16).

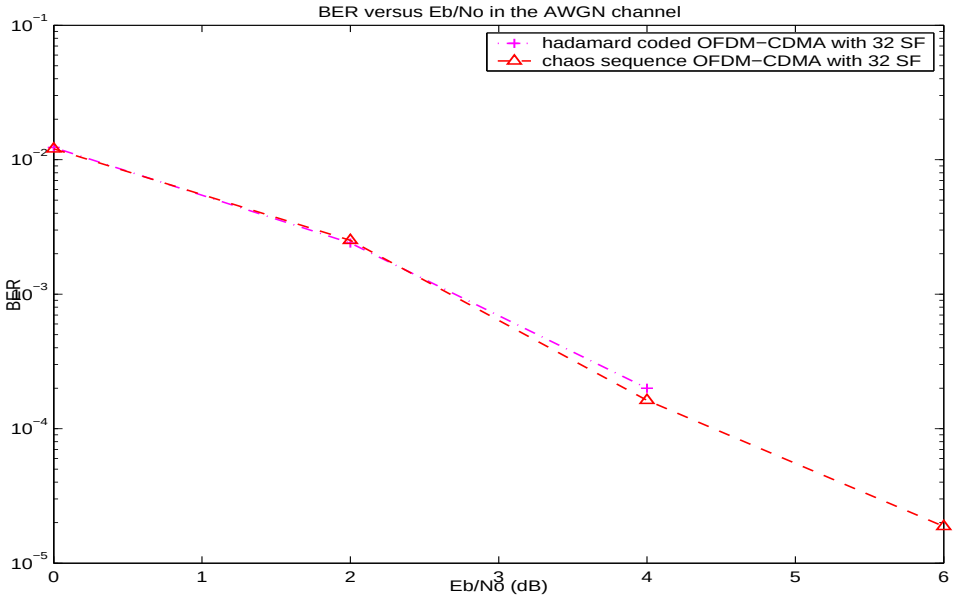

Figure 5.17: BER performance for the chaos-based and the PN-based OFDM-CDMA in AWGN (SF=32, FFT size = 16).

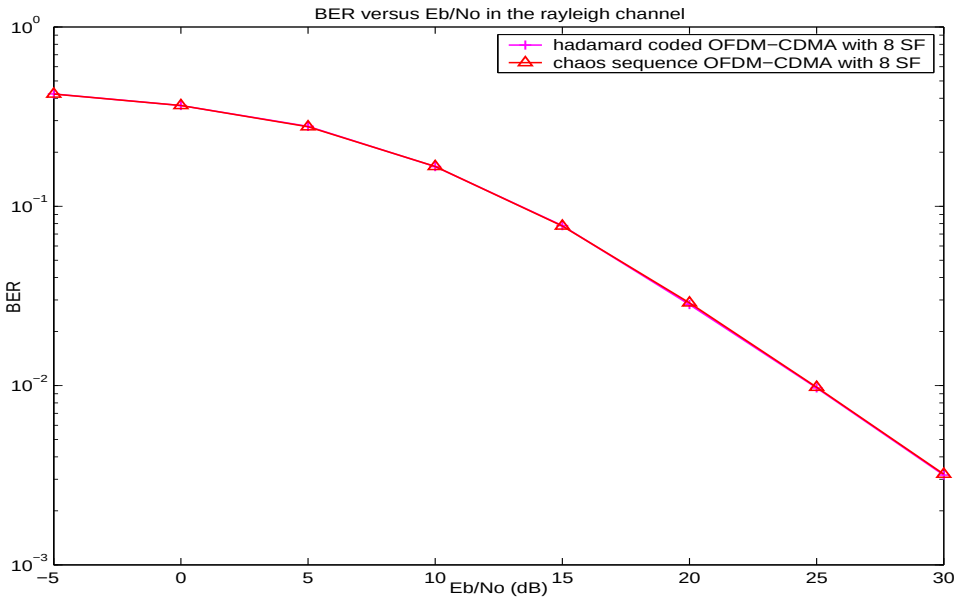

Figure 5.18: BER performance for the chaos-based and the PN-based OFDM-CDMA in Rayleigh channel (SF=8, FFT size = 16).

5.4.2 Rayleigh Fading Channel

In this simulation, we assume that the receiver and the transmitter are in stationary condition (flat fading), and no Doppler shift is applied. The received signal after OFDM demodulation is assumed to have perfect channel estimation:

$$r_n = \text{FFT}((\text{IFFT}(s_n)h_n + \eta_n)h_n^*) \tag{5.12}$$

where h_n^* is the complex conjugate of h_n.

Figures (5.18, 5.19 and 5.20) show the BER performance for the uncoded chaos-based OFDM-CDMA and the uncoded PN-based OFDM-CDMA in the Rayleigh fading channel with AWGN. As in the case of Rayleigh fading and

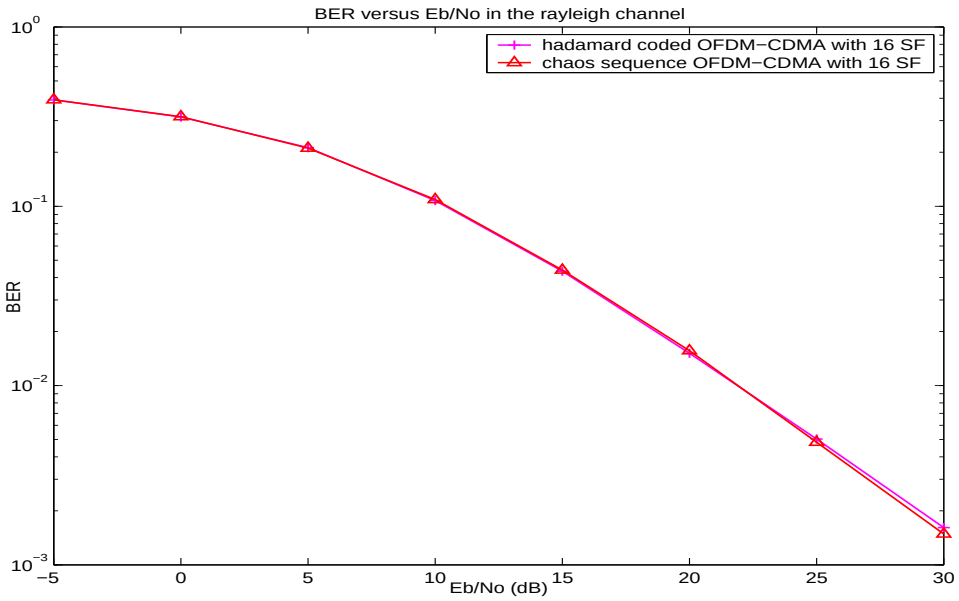

Figure 5.19: BER performance for the chaos-based and the PN-based OFDM-CDMA in Rayleigh channel (SF=16, FFT size = 16).

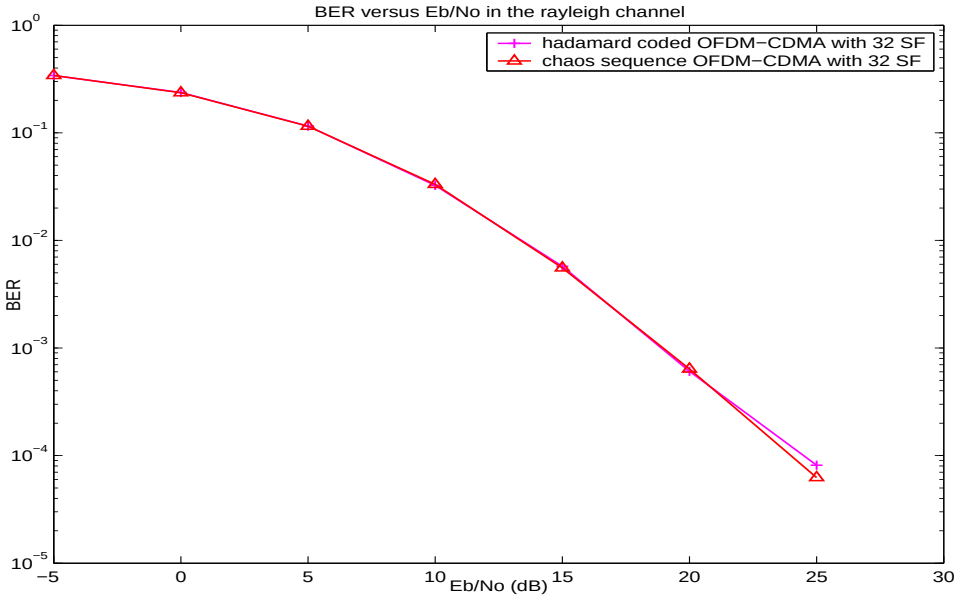

Figure 5.20: BER performance for the chaos-based and the PN-based OFDM-CDMA in Rayleigh channel (SF=32, FFT size = 16).

AWGN channel conditions, there is nearly no performance advantage for either system over the other. Both chaos-based and PN-based OFDM-CDMA systems provide similar BER performance. However, chaos-based OFDM-CDMA has a major performance advantage over PN-based OFDM-CDMA where it provides higher security at the physical link layer.

5.4.3 Discussion

We presented a comparative study between two OFDM-CDMA communication systems: one utilizing a simple recursive chaotic sequence and the other utilizing a PN sequence for spreading. Both systems showed nearly similar bit-error-rate (BER) performance under all channel conditions. On the other hand, the chaotic-based system has significant advantages over the PN-based system as the former allows a higher number of users and provides more secure communication.

5.4.4 Conclusions

In this chapter we presented three different MCM techniques for chaos communication. In the first section, studied the use of chaos shift keying in conjunction with both OFDM (CSK-OFDM) and Wavelet OFDM (WOFDM) systems (CSK-WOFDM), where wavelet-based method (CSK-WOFDM) provided performance advantage over CSK-OFDM as well as increased the security prospective of the system. Lower PAPR value and higher bandwidth efficiency are also shown to be provided by CSK-WOFDM system. In the second section, we pro-

vided a comparative study for conventional CDMA and chaotic-based CDMA. Theoretically, the chaotic sequences are unlimited in length, and are suitable for a large number of users. Again, due to bifurcation behavior of a chaotic generator, chaotic sequences can be useful for secure communications, as it is practically impossible to predict a chaotic pattern on long term. Last section showed a comparative study between OFDM-CDMA communication systems and chaos-based CDMA-OFDM scheme. This section is an extension to the second section, where both PN-based and chaos-based CDMA are used in conjunction with OFDM. Both systems showed nearly similar bit-error-rate (BER) performance under all channel conditions. Again, the chaotic-based system has significant advantages over the PN-based system as the former allows a higher number of users and provides more secure communication.

Chapter 6

Blind Adaptive Multiuser Detection for Chaos CDMA Communication

6.1 Introduction

During the past decade, intensive research in modelling non-linear dynamic systems provided a possibility to approach these non-linear systems using chaos theory. Research in this area had uncovered the beauty of a mixture of deterministic and dynamic stochastic behaviors of chaotic systems. Interestingly, this has unfolded several common signal properties to the communication engineering problem, such as the use of random noise-like behavior of the chaotic system in both analog and digital spread spectrum communications [7, 17, 77, 103]. In digital communications, chaotic systems can be used in code-level optimization of a code-division multiple access (CDMA) and have proven to be superior to the classical approaches in many realistic environments [103], particularly in combatting the multiple access interference (MAI) [103, 104, 105, 106].

Multiple access wireless communication systems employ different methods to multiplex different users for transmission over one wireless channel. There

were two major schemes that had been widely used in the past: frequency division multiple access (FDMA) and time division multiple access (TDMA), both were used in first and second generation wireless mobile communications. FDMA systems assigned a distinct orthogonal frequency for each user, while TDMA systems employed orthogonal time slots for users. However, in the new generation of wireless communications, a code division multiple access (CDMA) is preferable. Spread spectrum (SS) CDMA communication is produced by directly multiplying the user information bits (in the time domain) by a known spreading sequence code running at a much higher rate to spread the user information over the bandwidth of the transmitted signal. In this way, it is expected that the detrimental effect of intentional jamming and interference arising from the inner-cell or outer-cell users can be suppressed.

In CDMA systems, the spreading code is generated using a pseudo-random noise (PN) generator or some specially-designed code generator, such as, Gold code, Kasami code, Walsh Hadamard, M-sequence and OVSF code [79]. However, these generators produce repeating sequences, which lead to a very predictable fashion. Therefore, they performed unsatisfactorily in terms of system capacity and security. Recent studies suggested that the use of chaos generators to generate the code sequence of CDMA systems [20, 78, 104, 105, 106] can increase the system capacity [103] and may also be used to address the security drawback in spread spectrum communication [7]. Furthermore, it is apparent that this sequence has the auto- and cross- correlation properties requested by spread spectrum systems. The beauty of chaos generator bifurcation behavior can provide a security aspect to the system, where the chaotic sequence is very sensitive to the initial condition chosen. Hence, an exact initial condition value must be known at the receiver side to be able to regenerate the CDMA code

for demodulation of the transmitted signal.

On the receiver side of CDMA communication systems, conventional detectors are usually employed (e.g., RAKE/Correlator receivers, and zero-forcing detectors). However, these schemes do not provide optimal solutions, particularly for multi-user detection systems. Digital signal processing may provide the solution, and adaptive filtering methods for the next generation of mobile communications have been considered [107] and [108]. This involves the development of blind adaptive systems, where training sequences are not required by the receiver. For example, in [109], the uniformly-distributed dithered signed-error constant modulus algorithm has been implemented for DS-CDMA multiuser detection. It was shown that the algorithm is able to lock each user to their specific set of minima, while retaining the averaged transient behavior of the constant modulus algorithm. For simplicity, we employ here the conventional constant modulus algorithm (CMA) for blind user detection. We will consider the DS-CDMA communication systems model with K users and provide a brief covering of the adaptive multiuser detection techniques and present a blind scheme constant modulus algorithm (CMA) for both conventional CDMA and Chaos-CDMA communication.

6.2 System Model

Figure (6.1) depicts the transmitter and receiver system model of a baseband DS-CDMA communication system with K users. Each user transmits binary symbols $s(n) \in \{-1, +1\}$ using BPSK modulation. The k^{th} user of the source symbol sequence with T_b symbol period, denoted by $s_k(n)$, is spread by a pseudo-noise code (or chaos code sequence) of length L with a chip du-

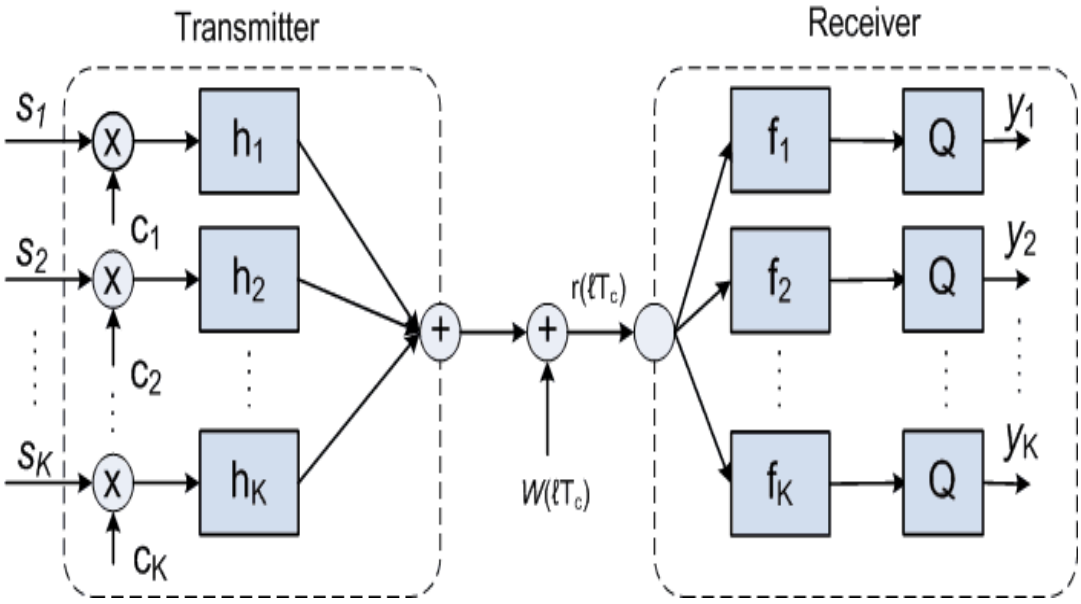

Figure 6.1: DS-CDMA communication system model with K users.

ration of T_c. Thus, the spreading gain of the system can be expressed as $L = T_b/T_c$. The spreading sequence of the k^{th} user can be written in vector form as $\mathbf{c}_k = [c_k(0), c_k(1), c_k(\ell), \ldots, c_k(L-1)]^t$, where $c_k(\ell) \in \{-1, +1\}$ and $(.)^t$ is a transpose operator. The coefficients of the k^{th} user channel are summarized in the vector $\mathbf{h}_k = [h_k(0), h_k(1), h_k(\ell), \ldots, h_k(N_h - 1)]^t$, where N_h denotes the channel length. The additive Gaussian noise process, $w(\ell T_c)$, is independent of the source symbols and has zero mean and variance σ_w^2. On the receiver part, a bank of correlators (or an adaptive filter) is used, followed by hard decision devises (Q) that are applied to produce hard decision output.

6.3 Chaotic Sequences

Refer to Chapter 5 for chaos-CDMA system and discussion. A non-linear chaos generator used to generate the chaotic spreading sequences is given by Chapter

5 as follows:

$$c_{n+1} = 1 - ac_n^2. \tag{6.1}$$

The initial value $c_o = c(0)$ for the system is taken from the open interval $(-1, 1)$. The chaos sequences is then past to a quantizer to convert the chaos sequence into a binary chaos-CDMA sequence.

6.4 Multiuser Detection Schemes

6.4.1 Correlator Filter Detection

The transmitted message from the k^{th} user at the chip duration ℓT_c is expressed as:

$$\mathbf{u}_k(\ell T_c) = \mathbf{H}_k \mathbf{C}_k \mathbf{s}_k(n). \tag{6.2}$$

where $\mathbf{H}_k$ denotes the channel convolution matrix:

$$\mathbf{H}_k = \begin{bmatrix} h_k(0)\, h_k(1) & \cdots & h_k(N_h - 1) & & \\ & \ddots & & \ddots & \\ & & h_k(0) & h_k(1) & \cdots\, h_k(N_h - 1) \end{bmatrix} \tag{6.3}$$

with a dimension of $N_f \times (N_f + N_h - 1)$; N_f being the equalizer length. The spreading code matrix $\mathbf{C}_k$ of dimension $(N_f + N_h - 1) \times N_s)$ is defined as:

$$\mathbf{C}_k = \begin{bmatrix} \mathbf{c}_k & & & \\ & \mathbf{c}_k & & \\ & & \ddots & \\ & & & \mathbf{c}_k \end{bmatrix}, \tag{6.4}$$

where the column vector $\mathbf{c}_k$, is a chip sequence of length L. Thus, the number of source symbols from the k^{th} user that are considered to estimate the output symbol at the time-index n may be given as:

$$N_s = \left\lceil \frac{N_f + N_h - 1}{L} \right\rceil. \tag{6.5}$$

Clearly, the source symbol vector will be as follows:

$\mathbf{s}_k(n) = [s_k(0), s_k(1), \ldots, s_k(n - N_s + 1)]^t$.

Finally, the received signal vector $\mathbf{r}(\ell T_c)$ at the input of the filter can be expressed as:

$$\begin{aligned} \mathbf{r}(\ell T_c) &= \sum_{k=1}^{K} \mathbf{u}_k(\ell T_c) + \mathbf{w}(\ell T_c) \\ &= \sum_{k=1}^{K} \mathbf{H}_k \mathbf{C}_k \mathbf{s}_k(n) + \mathbf{w}_k(\ell T_c) \\ &= [\mathbf{H}_1\mathbf{C}_1 \ \mathbf{H}_2\mathbf{C}_2 \ \ldots \ \mathbf{H}_K\mathbf{C}_K] \begin{bmatrix} \mathbf{s}_1(n) \\ \mathbf{s}_2(n) \\ \vdots \\ \mathbf{s}_K(n) \end{bmatrix} \\ &\quad + \mathbf{w}(\ell T_c). \end{aligned} \tag{6.6}$$

Assuming perfect channel estimation, the soft decision correlator detector output for each user is formulated as follows:

$$\hat{y}_k(n) = \mathbf{r}^t(\ell T_c)\mathbf{H}_k^*\mathbf{C}_k. \tag{6.7}$$

6.4.2 Adaptive Filter Detection

The soft linear detector output for each user is computed at symbol rate from the received vector $\mathbf{r}(\ell T_c) = [r(1), r(2), \ldots, r(\ell T_c - N_f + 1)]^t$ as follows:

$$\hat{y}_k(n) = \mathbf{f}_k^t \mathbf{r}(\ell T_c). \tag{6.8}$$

In blind systems utilizing CMA, adaptation of the filter coefficients using the gradient descent method can be expressed as follows:

$$\mathbf{f}(n+1) = \mathbf{f}(n) + \varphi \mathbf{r}(n) \psi_{\text{cma}}(y_n), \tag{6.9}$$

where φ is a small positive step-size, and $\psi_{\text{cma}}(y_n)$ is the CMA error function. The error function may be formulated as :

$$\psi_{\text{cma}}(y_n) \equiv y_n^*(\gamma - \mid y_n \mid^2), \tag{6.10}$$

where γ is a dispersion constant defined as $\gamma \equiv E[|s_n|^4]/E[|s_n|^2]$. Under the condition of perfect blind equalization (PBE) [110], equalizers minimizing the CM cost function can perfectly recover the original source symbols for some values of the system delay δ [where $0 \leq \delta \leq N_s - 1$] such that $y_n = s_{n-\delta}$. In the same direction, the adaptive multiuser detection filters are also considered as equalizers. Therefore, this blind adaptive algorithm may be employed to estimate the transmitted symbol sequence of each user.

It should be noted that, since the CMA cost-surface has multi-modal properties [110], a set of minimum points exists. Therefore, in a multiuser system with K users, K sets of minima exist. Each minimum point of a specific set of minima relates to a different delay. Depending on the channel characteristics

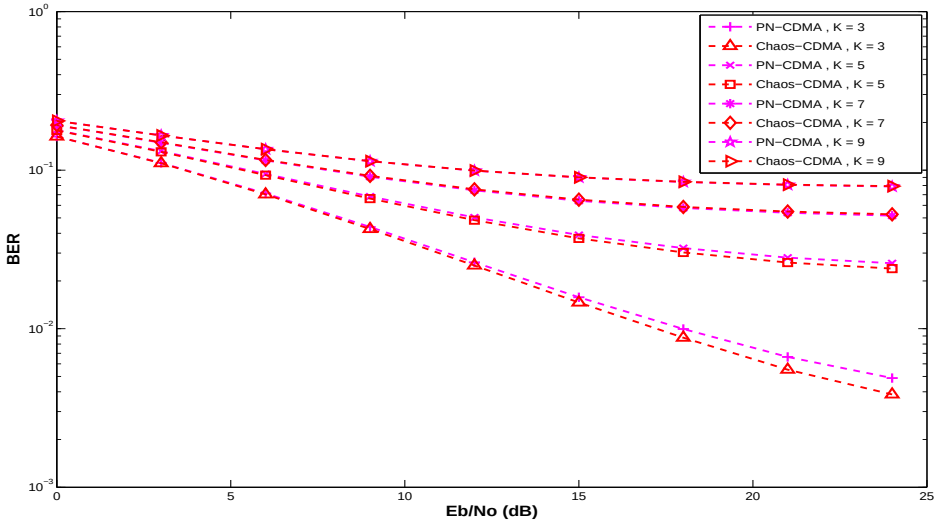

Figure 6.2: BER performance of the chaos-based and PN-based CDMA with spreading gain (spreading factor) L=16 in a Rayleigh fading environment. The received signal is decoded using a correlator filter detector.

and noise distortion, their depth can also vary widely. From this point of view, adaptive multi-user detection refers to the algorithm capability to lock one user to its set of minima and converge to those points. If the algorithm leads to the wrong set of minima, it directs the decision to the wrong user.

6.5 Simulation Results

For correlation detection, the multiuser CDMA system was simulated for different number of users in a wireless Rayleigh environment over 500 realizations. We assumed that the receiver has a perfect channel estimation.

Figures (6.2) - (6.4) show the BER performance of the chaos-based and PN-based CDMA systems using a correlator, with spreading gains (spreading factors) of L=16, L=32, and L=64 in a Rayleigh fading environment. Generally, the chaos-based CDMA provides better BER performance than the PN-based

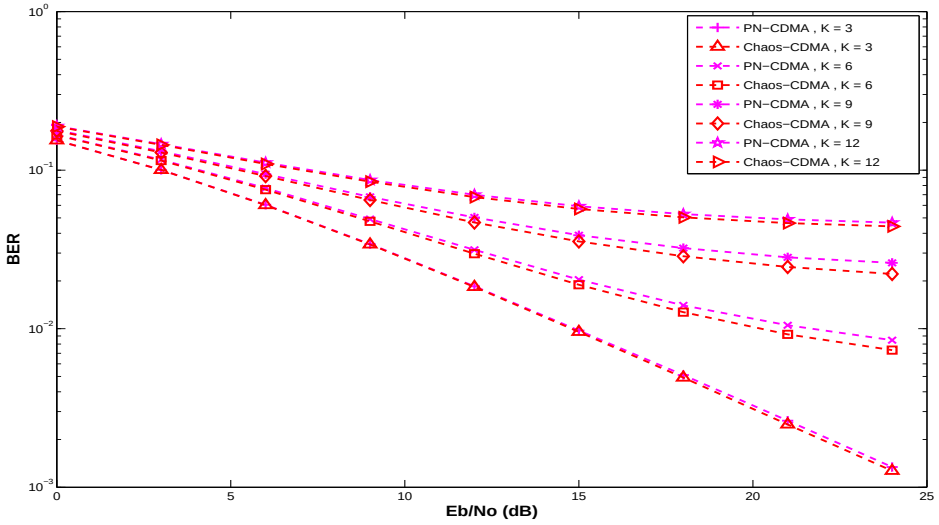

Figure 6.3: BER performance of the chaos-based and PN-based CDMA with spreading gain (spreading factor) L=32 in a Rayleigh fading environment. The received signal is decoded using a correlator filter detector.

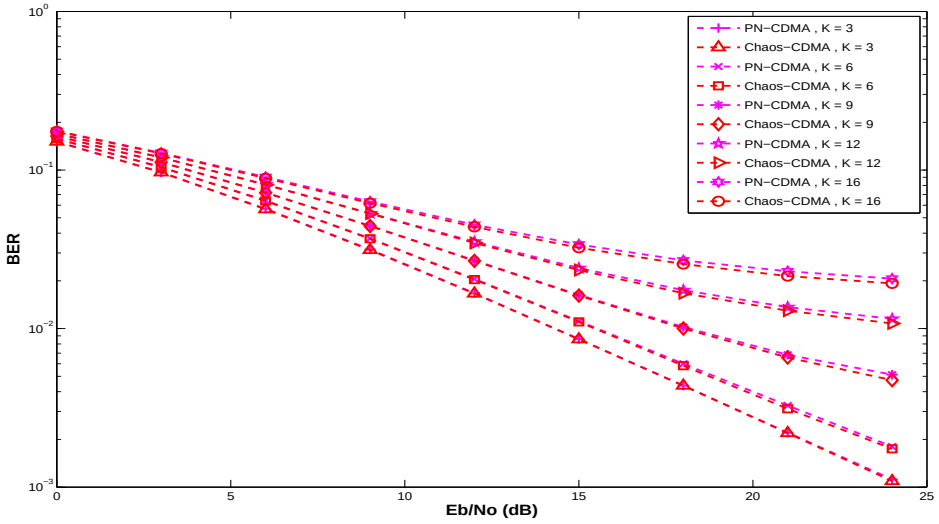

Figure 6.4: BER performance of the chaos-based and PN-based CDMA with spreading gain (spreading factor) L=64 in a Rayleigh fading environment. The received signal is decoded using a correlator filter detector.

CDMA. It is worth noting that the performance of chaos-based CDMA is better than that of PN-based CDMA for a lower number of multiusers at a lower spreading gain (spreading factor), and for a higher number of multiusers at a higher spreading gain (spreading factor). There is no performance gain otherwise.

The adaptive multiuser detection on CDMA system was simulated for different number of users in the same cell and different spreading gains for both chaos and PN sequences. Dispersion constant γ was set to 1 for BPSK modulation. The algorithm step-size (φ) was set to 8×10^{-4} when the number of users was 16 and $\varphi = 5 \times 10^{-4}$ when the number of users was 8. The filter length N_h was set to $2L$. Along the way from transmitter to receiver, white Gaussian noise is added and it was assumed that Signal to Noise ratio (SNR) of 40 dB. Where signal power is $\varepsilon\{x\}^2$, noise power is $No/2$ and $|x|^2$ is normalized to one, The mean-squared error trajectories in all cases were averaged over 100 Monte Carlo iterations.

In figure (6.5), the number of users (K) in the cell was set to 8 and the spreading gain of the code sequences was set to L =64. The figure depicts the individual mean-squared error trajectory of each user. It is shown that each user was locked at a different value of MSE for both sequences. The convergence speed of the filter coefficients adaptation taken from the average MSE of all users for different spreading codes is plotted in figure 6.7 (bottom). It can be seen clearly that CDMA system utilizing chaos sequences outperforms the PN-based CDMA in terms of convergence speed, with the same MSE for chaos and PN code sequences.

Increasing the number of users in the cell to K =16 gives the same performance as above. The averaged MSE trajectories for individual users are shown

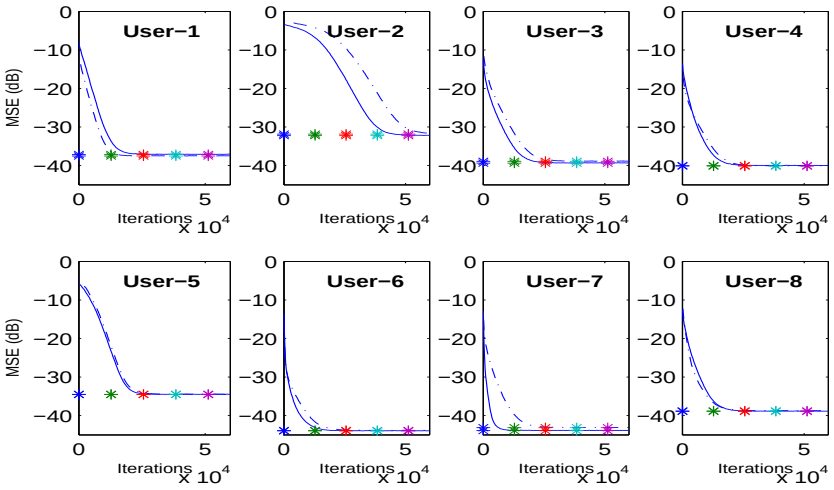

Figure 6.5: Individual averaged mean-squared error (MSE) trajectories of adaptive filters. Chaos-based (− line) and PN-based (−. line) CDMA, K =8 users, spreading gain (spreading factor) L=64.

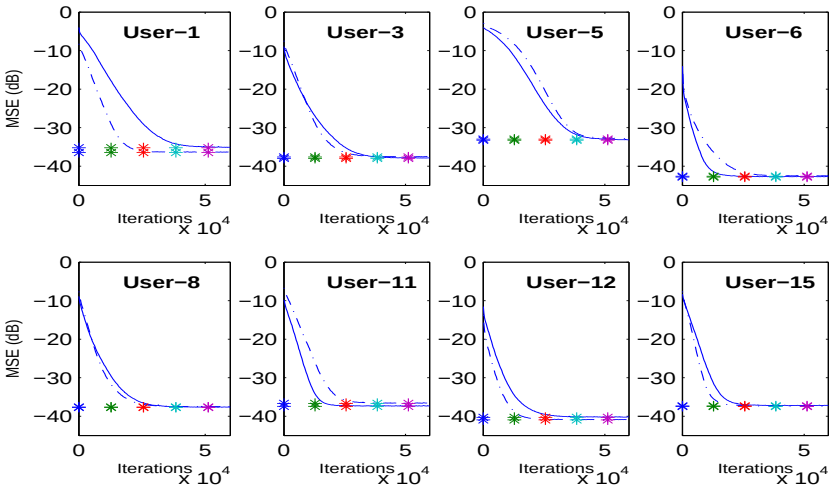

Figure 6.6: Individual averaged mean-squared error (MSE) trajectories of adaptive filters. Chaos-based (− line) and PN-based (−. line) CDMA, K =16 users, spreading gain (spreading factor) L =64.

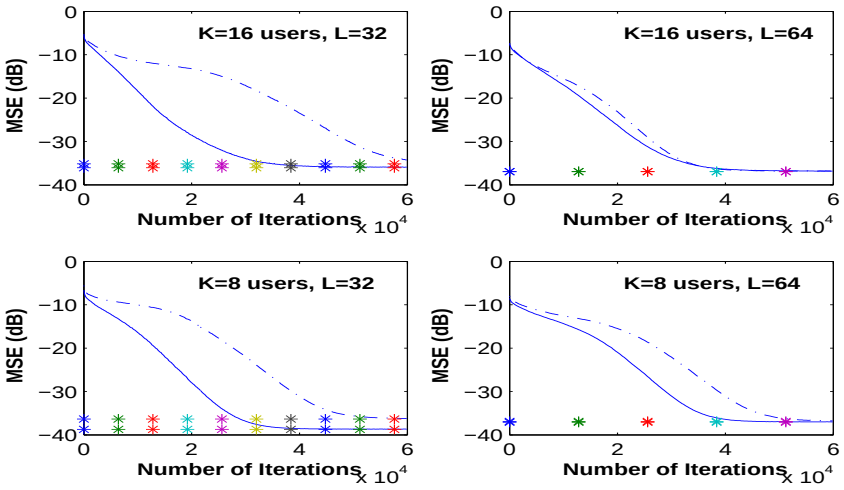

Figure 6.7: Averaged mean-squared error trajectories taken from the average value of the K users. Chaos-based ($-$ line) and PN-based ($-.$ line) CDMA, different number K users and different values of spreading gain (L).

in figure (6.6), while the average MSE of all users for different spreading codes are plotted in figure 6.7 (top).

6.6 Conclusion

The use of blind adaptive constant modulus algorithm for multiuser detection is studied in this chapter, where the transmitted signal is spread by chaos-based sequences for CDMA. A comparison with PN-based CDMA in multiuser detection showed that the chaos-based CDMA sequences do provide enhancement in terms of BER and MSE for both detection schemes (matched filtering/correlator detection and adaptive filter detection). Further study is needed to examine the use of CMA for chaos-CDMA in different channel environments.

Chapter 7

Weight-Vector LMS Algorithms for Adaptive Beamforming in Chaos Communication

7.1 Introduction

Wireless signals sent from an RF transmitter experience not only propagation loses of the electromagnetic wave power, but also geometrical effects that result in multipath components and angle spread [111, 112, 12]. These paths result from the reflection, diffraction or scattering of the signal over objects that lie in the environment, like buildings or natural scatterers. In other words, the signal received at the antenna will contain the transmitted signal as well as some unwanted signals at different angles of arrival. By using beamforming techniques, we can direct the radiated power towards the desired signal and null the interfering signals [111, 112]. This will result in the increase of signal to interference ratio (SIR) and lead to better signal estimation. In adaptive beamforming, the adaptive LMS algorithm provides the optimum solution for the antenna weights vector and results in minimizing the mean-square error (MSE) between the beamforming output and the desired signal.

The LMS algorithm is a well-known adaptive estimation and prediction technique. It has extensively been studied. Despite its simplicity, the LMS algorithm is capable of achieving a satisfactory performance which converges to the optimum Wiener solution [71, 72, 111]. The LMS has the ability to predict and estimate a wide range of signals, including polynomial signals. Since a logistic chaos signal can be considered as a non-linear polynomial signal, we will study the possible use of adaptive beamforming algorithms in chaos communications.

In this chapter, we propose two structures for adaptive LMS algorithm, the fixed forward prediction WV-LMS (FWV-LMS) and the updated forward prediction WV-LMS (UWV-LMS), and apply them in a beamforming technique for two different transmitted signals. It is known that the performance of the conventional LMS algorithm is dependent on the signal condition and the chosen convergence parameter μ. The parameter μ in the conventional LMS algorithm is fixed, while the proposed algorithms dynamically change the convergence parameter μ_n depending on the forward prediction of the weights vector. This change in the convergence parameter provides another level of adaptability to the changes in wireless channel environment. These algorithms are tested for two different non-linear transmitted signal: non-linear quadratic frequency modulated (QFM) and logistic map chaos shift keying (CSK) signal. Under both signal conditions, the proposed algorithms have shown to provide performance improvement in terms of the mean squared error (MSE).

7.2 Least-Mean Square Adaptive Algorithm

In the conventional adaptive LMS algorithm, the coefficients (weights vector) $\mathbf{w}(n)$ of the FIR filter are updated according to the following formula [71, 72]:

$$\mathbf{w}(n) = \mathbf{w}(n) + \mu e(n)\mathbf{y}(n) \tag{7.1}$$

where $\mathbf{w}(n) = [w_o(n) \;\; w_1(n)...w_M(n)]$ ($M+1$ being the filter length), μ is the convergence parameter (sometimes referred to as *step-size*), $e(n) = d(n) - z(n)$ is the output error ($z(n)$ being the filter output), and $d(n)$ is the reference signal. Note that $z(n) = \mathbf{w}(n)\mathbf{y}^T(n) = \hat{x}(n)$, where $\hat{x}(n)$ is the original signal and $\mathbf{y}(n) = [y(n) \;\; y(n-1)...y(n-M)]$ is the filter input signal.

7.3 Proposed Weights Vector LMS algorithms

The weights vector in the beamforming algorithm controls the beam radiation direction. In the conventional LMS beamforming algorithm, we utilize the feedback information ($e(n)$ the output error) to forward-predict the new weights vector $\mathbf{w}(n+1)$. This new weights vector tells the antenna array where the beam should be directed in time $n+1$. Hence, the system should improve if the new weights vector are fedback to the system for further prediction. The two proposed algorithms used this forward predicted weights vector and current weights vector to generate a new parameter ϵ_n using the difference between the norm of both weights vectors as shown below:

$$\epsilon_n = \frac{\parallel \mathbf{w}(n+1) - \mathbf{w}(n) \parallel}{\parallel \mathbf{w}(n+1) \parallel} \tag{7.2}$$

the ϵ_n is then passed to the alpha filter to generate the new convergence parameter μ_{n+1} that will be used to predict the weights vector $\mathbf{w}(n+1)$:

$$\mu_{n+1} = \begin{cases} \alpha\mu_n + \delta\epsilon_n & \text{, if } 0 < \mu_{n+1} < \mu_{\max} \\ \mu_{\max} & \text{, otherwise} \end{cases} \tag{7.3}$$

where $\mu_{\max}$ is the maximum convergence parameter that can be used for LMS algorithm, and $\mu_{\max}$ is defined as [71, 72]:

$$\mu_{\max} < \frac{2}{\lambda_{\max}} \tag{7.4}$$

where $\lambda_{\max}$ is the largest eigenvalue of the correlation matrix of the signal [71, 72]. The forward prediction convergence parameter μ can be a fixed value (like LMS algorithm) named as *fixed forward WV-LMS (FWV-LMS)* in this Thesis, or a dynamic convergence parameter μ_n, named as *updated forward prediction WV-LMS (UWV-LMS)*.

7.3.1 Fixed Forward Prediction WV-LMS (FWV-LMS)

In the fixed forward prediction WV-LMS, a conventional LMS with a fixed convergence parameter μ is used to forward prediction of the weights vector $\mathbf{w}(n+1)$. New convergence parameter μ_{n+1} is then calculated from the $\mathbf{w}$(n+1). The weights vector $\mathbf{w}$(n+1) will be recalculated using the new convergence parameter μ_{n+1}. An outline of the FWV-LMS algorithm is shown in the following

steps:

$$
\begin{aligned}
z(n) &= \mathbf{w}(n)\mathbf{y}^T(n) \\
e(n) &= d(n) - z(n) \\
\mathbf{w}(n+1) &= \mathbf{w}(n) + \mu_{\text{fix}} e(n)\mathbf{y}(n) \\
\epsilon_n &= \frac{\parallel \mathbf{w}(n+1) - \mathbf{w}(n) \parallel}{\parallel \mathbf{w}(n+1) \parallel} \\
\mu_{n+1} &= \begin{cases} \alpha\mu_n + \delta\epsilon_n & \text{, if } 0 < \mu_{n+1} < \mu_{\max} \\ \mu_{\max} & \text{, otherwise} \end{cases} \\
\mathbf{w}(n+1) &= \mathbf{w}(n) + \mu_{n+1} e(n)\mathbf{y}(n)
\end{aligned}
$$

where ^{T} indicates matrix transposition.

7.3.2 Updated Forward Prediction WV-LMS (UWV-LMS)

The updated forward prediction WV-LMS works in the same way as the FWV-LMS. However, it will forward-predict the weights vector using the updated μ_n. An outline of the UWD-LMS algorithm is shown in the following steps:

$$
\begin{aligned}
z(n) &= \mathbf{w}(n)\mathbf{y}^T(n) \\
e(n) &= d(n) - z(n) \\
\mathbf{w}(n+1) &= \mathbf{w}(n) + \mu_n e(n)\mathbf{y}(n) \\
\epsilon_n &= \frac{\parallel \mathbf{w}(n+1) - \mathbf{w}(n) \parallel}{\parallel \mathbf{w}(n+1) \parallel} \\
\mu_{n+1} &= \begin{cases} \alpha\mu_n + \delta\epsilon_n & \text{, if } 0 < \mu_{n+1} < \mu_{\max} \\ \mu_{\max} & \text{, otherwise} \end{cases} \\
\mathbf{w}(n+1) &= \mathbf{w}(n) + \mu_{n+1} e(n)\mathbf{y}(n.)
\end{aligned}
$$

7.4 Adaptive Beamforming

In a uniformly spaced linear antenna array, the desired signal arrives at the antenna array with an angle θ_0 and the i^{th} interfering signal $u_i(t)|i = 1, ...N_u$ arrive with an angle θ_i, where N_u is the number of interfering signals. The output of the linear antenna array can be formulated as follows [111]:

$$\mathbf{x}(t) = s(t)\mathbf{v} + \mathbf{u} = \mathbf{s} + \mathbf{u} \tag{7.5}$$

where $\mathbf{v}$ is the array propagation vector for desired signal:

$$\mathbf{v}^T = [1, e^{j2\pi d \sin\theta_0/\lambda}, ...e^{j(K-1)2\pi d \sin\theta_0/\lambda}] \tag{7.6}$$

where K is the number of elements in the antenna array and $\mathbf{u}$ represents the sum of all interfering signal vectors [111]:

$$\mathbf{u} = \sum_{i=1}^{N_u} u_i(t)\eta_i \tag{7.7}$$

η_i is the array propagation vector for the i^{th} interfering signal:

$$\eta_i^T = [1, e^{j2\pi d \sin\theta_i/\lambda}, \cdots, e^{j(K-1)2\pi d \sin\theta_i/\lambda}]. \tag{7.8}$$

Figure (7.1) shows the generic adaptive beamforming system. The beamforming output $\hat{s}(t) = \mathbf{w}^H\mathbf{x}(t)$ (referred as $z(n)$ in Sections II and III) is optimized (by minimizing the difference with the desired signal) using the LMS adaptive algorithm.

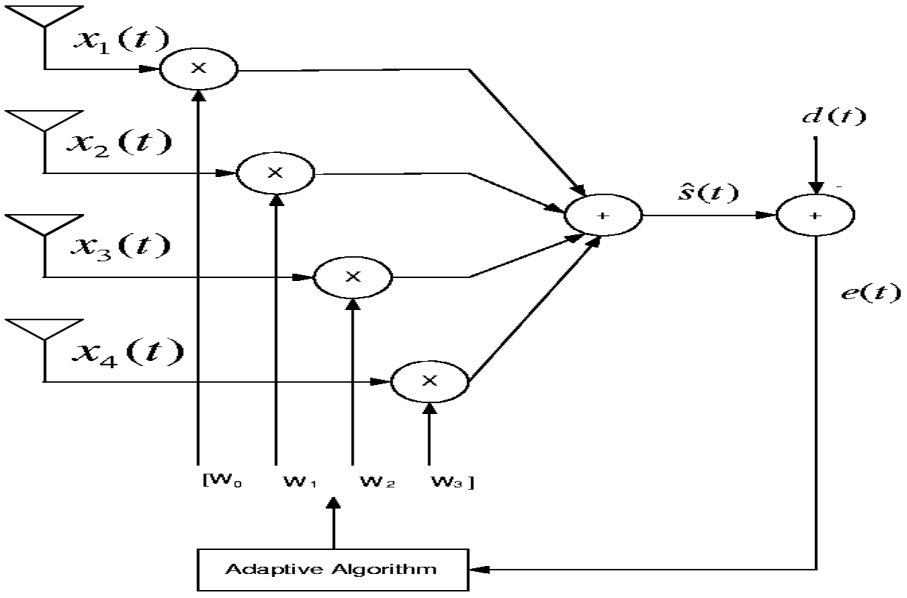

Figure 7.1: A generic adaptive beamforming system.

7.5 Simulation Results

We assume that the desired signal $s(t)$ is known to the receiver, hence reference signal is $d(n) = s(n)$. The interference signals at the receiver are assumed to be a Rayleigh fading type. The weights for the antenna array elements will be the coefficients of the FIR filter in the adaptive algorithm. The weights are updated using the equation in Section 7.3. To ensure no out of bound condition for all algorithms, the relation $\mu_{\max} = \mu_{\text{fix}} = 3\mu$ is used in this simulation. The mean squared error (MSE) is used as a performance measure of the beamforming system and is calculated as follows:

$$MSE = \frac{1}{N}\sum_{n=0}^{N}[s(n) - \hat{s}(n)]^2. \tag{7.9}$$

7.5.1 Quadratic Frequency Modulated (QFM) Signals

Many real-life and synthetic information-bearing signals can be frequency-modulated (linear, non-linear, or combinations of both). As a starting point, we perform our simulations using a narrow band non-linear FM signal as follows:

$$s(t) = \cos(\omega_o t + \gamma t^2/2 + \beta t^3/3)\Pi_T(t - T) \tag{7.10}$$

where $\omega_o = 2\pi f_o$ is a constant (initial frequency), T is the signal duration, and γ and β are the modulation indices which determine the bandwidth of the quadratic frequency modulated (QFM) signal. Similar results can be obtained using broadband CSK signals.

The bandwidth BW of this QFM signal can be adjusted by varying the parameters γ and β using the following relationships [113]:

$$f_m = \frac{1}{2\pi}\frac{\int_0^\infty \omega|X(\omega)|^2 d\omega}{\int_0^\infty |X(\omega)|^2 d\omega} \tag{7.11}$$

$$BW = \frac{1}{2\pi}\int_0^\infty (\omega - \omega_m)^2|X(\omega)|^2 d\omega \tag{7.12}$$

where $X(f)$ is the Fourier transform of $x(t)$ and f_m is its mean frequency. In this case, xt is the transmitted signal $s(t)$

Figure (7.2) shows the spectrum of a QFM narrow-band signal with $f_o = 100$ Hz, $\alpha = 0.5$, and $\beta = 0.37$.

Figures (7.3) and (7.4) show the MSE performance of the LMS, FWV-LMS and UWV-LMS beamforming for four antennas using a non linear FM signal in a low SIR (-10dB) environment. Figures (7.3) and (7.4) show that the performance is dependent on the choice of algorithm. WV-LMS algorithms provide better MMSE performance and always converges close to MMSE. The

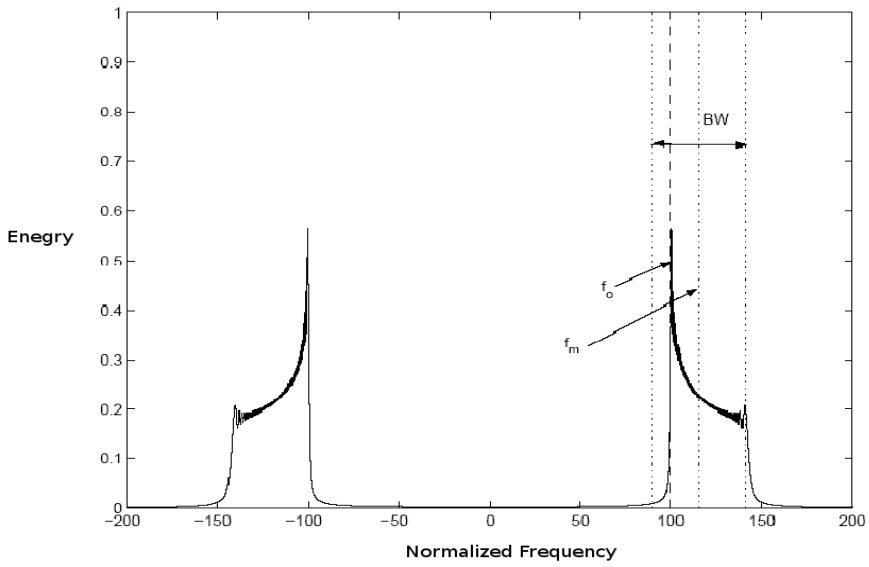

Figure 7.2: Spectrum of a QFM narrow-band signal with $f_o = 100$ Hz, $\gamma = 0.5$, and $\beta = 0.37$. bandwidth = 50 Hz.

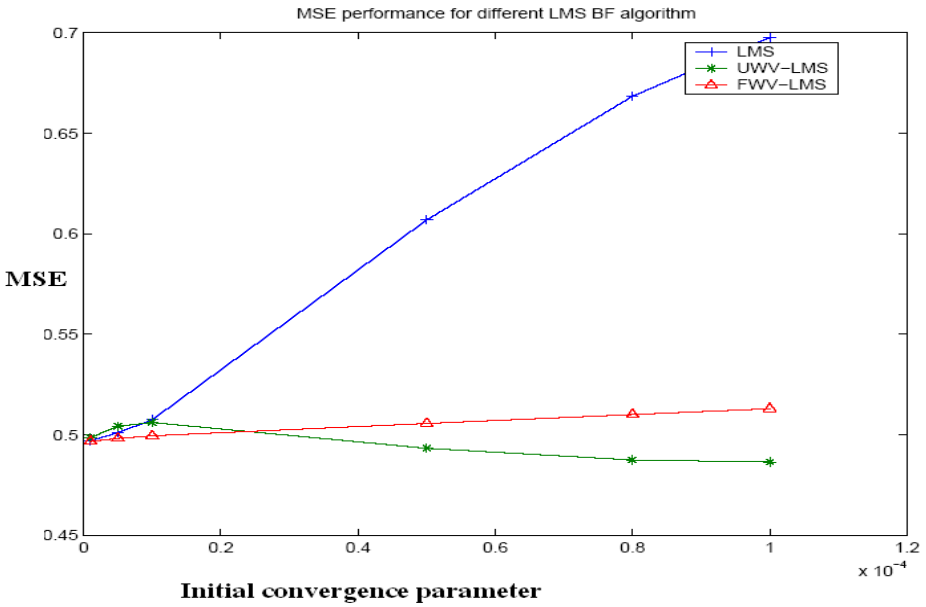

Figure 7.3: MSE performance for adaptive beamforming in QFM signal (4 antenna, SIR=[-10, -10], $\theta_i = [-30, 50]$, SNR = 10, BW = 200Hz, $\alpha = 0.95$, $\delta = 0.00003$).

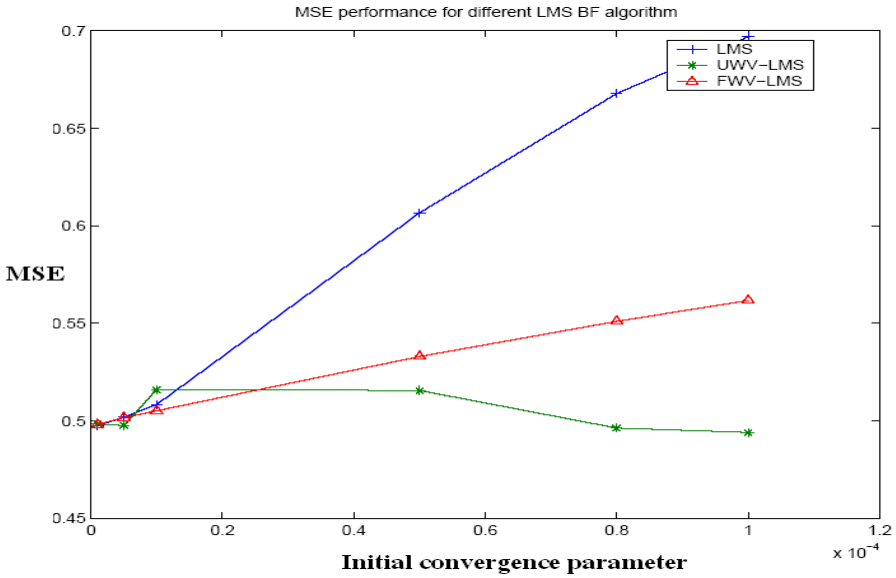

Figure 7.4: MSE performance for adaptive beamforming in QFM signal (4 antennas, SIR=[-10, -10], $\theta_i = [-30, 50]$, SNR = 10, BW = 200 Hz, $\alpha = 0.90$, $\delta = 0.0003$).

UWV-LMS also proved to be more adaptable to environment changes, while the FWV-LMS algorithm has better MSE performance than the conventional LMS algorithm.

Figures (7.5) and (7.6) show the MSE performance of the LMS, FWV-LMS and UWV-LMS beamforming with 4 antennas using a non-linear FM signal with a higher SIR (0dB) environment. The graphs show identical performance at low SIR environment as shown in figures (7.3) and (7.4). WV-LMS algorithms provide better MMSE performance. The UWV-LMS also proved to be more adaptable to the environment change.

Figures (7.7) and (7.8) show the MSE performance of the LMS, FWV-LMS and UWV-LMS beamforming with 2 antennas using a non-linear FM signal. Under both high and low SIR conditions, the graphs show identical advantage for the 4 antennas system. Both of the proposed algorithms provide better

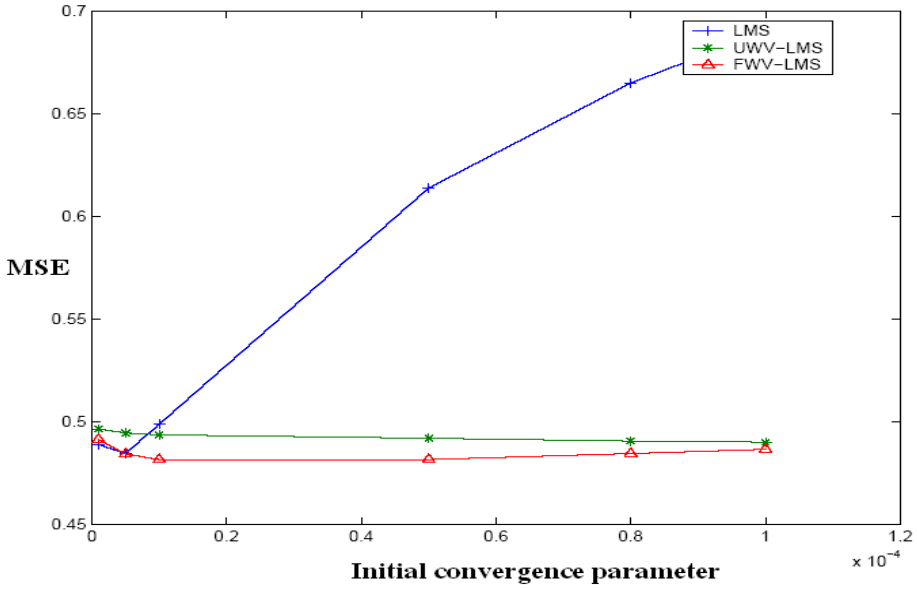

Figure 7.5: MSE performance for adaptive beamforming in QFM signal (4 antennas, SIR=[0, 0], $\theta_i = [-30, 50]$, SNR = 10, BW = 200 Hz, $\alpha = 0.95$, $\delta = 0.00003$).

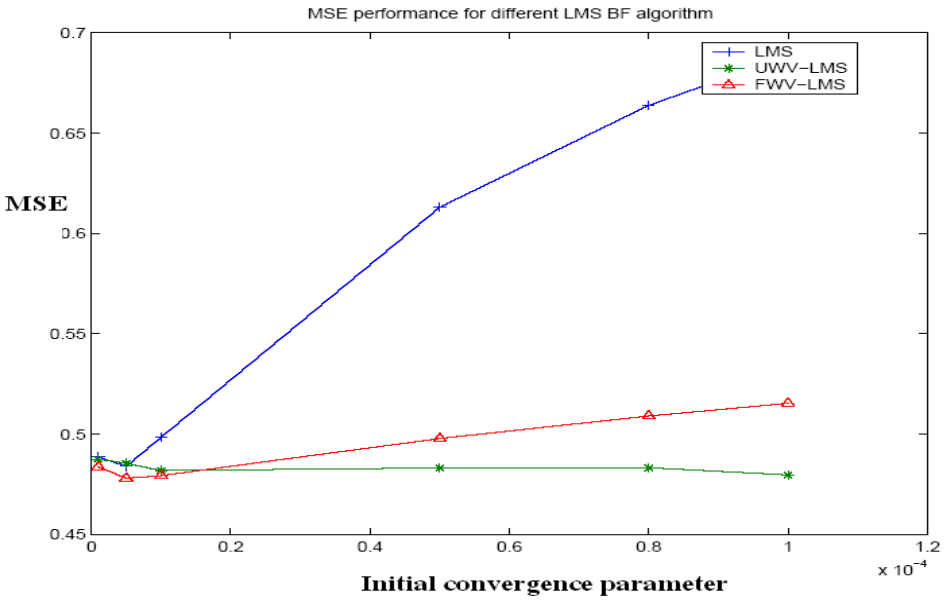

Figure 7.6: MSE performance for adaptive beamforming in QFM signal (4 antennas, SIR=[0, 0], $\theta_i = [-30, 50]$, SNR = 10, BW = 200 Hz, $\alpha = 0.90$, $\delta = 0.0003$).

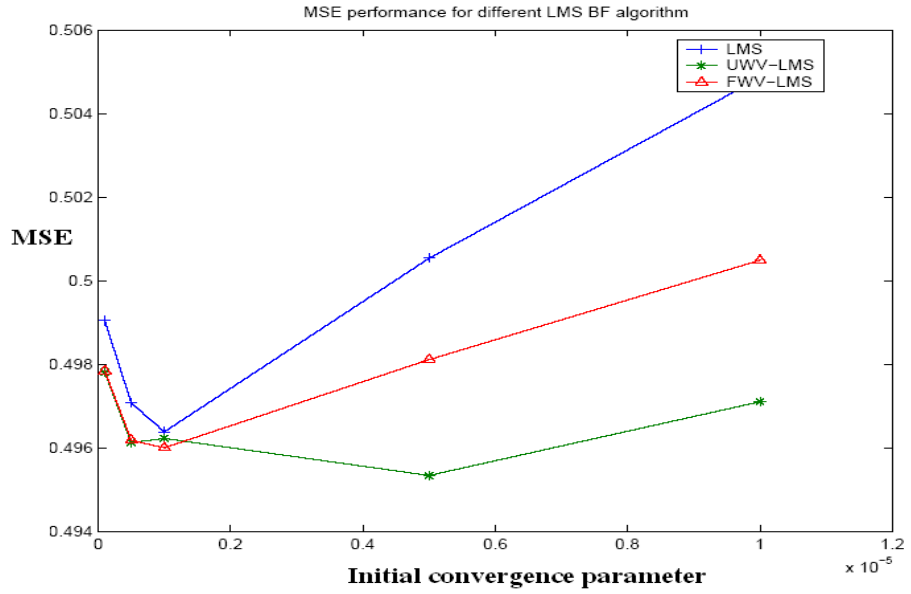

Figure 7.7: MSE performance for adaptive beamforming in QFM signal (2 antennas, SIR=[-10, -10], $\theta_i = [-30, 50]$, SNR = 10, BW = 200 Hz, $\alpha = 0.95$, $\delta = 0.00003$).

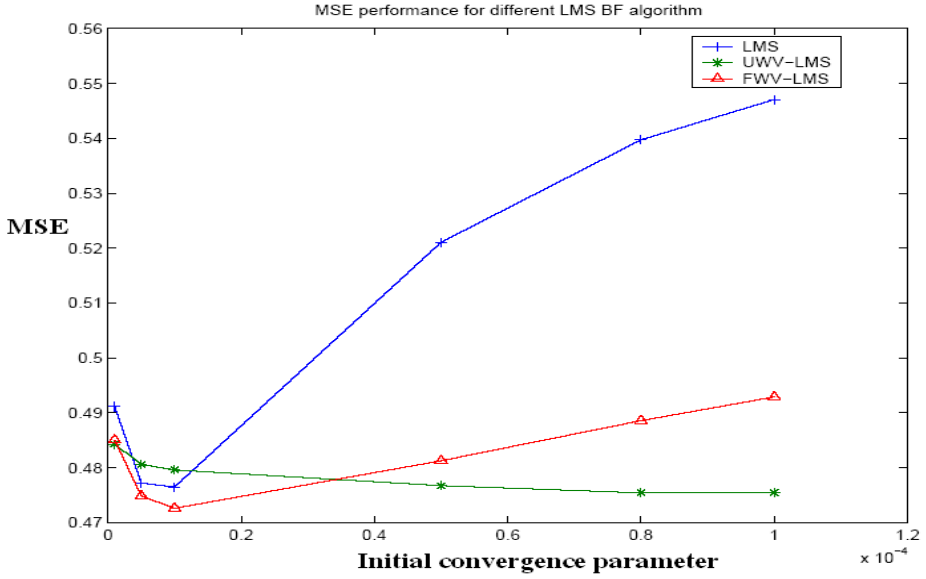

Figure 7.8: MSE performance for adaptive beamforming in QFM signal (2 antennas, SIR=[0, 0], $\theta_i = [-30, 50]$, SNR = 10, BW = 200 Hz, $\alpha = 0.90$, $\delta = 0.0005$).

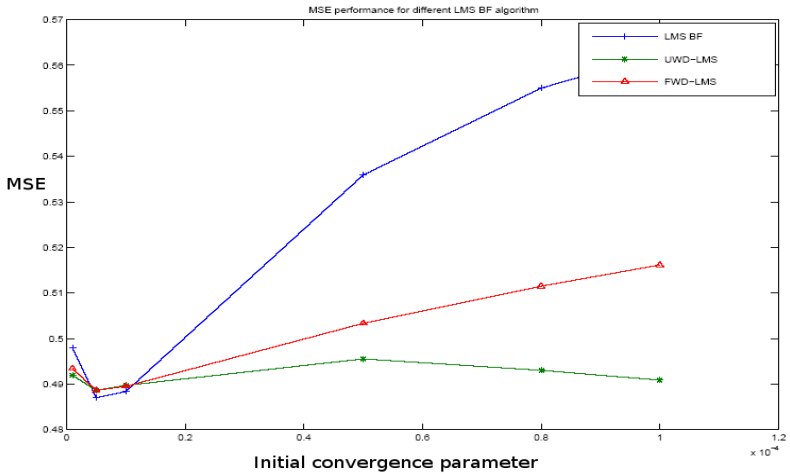

Figure 7.9: MSE performance for adaptive beamforming in CSK signal (2 antennas, SIR=[-10, -10], $\theta_i = [-30, 50]$, SNR = 10, $\alpha = 0.90$, $\delta = 0.0005$).

MMSE performance.

7.5.2 Chaos Shift Keying(CSK) Signals

A simple logistic map is used to generate CSK signal as shown in Chapter 3. Since, we are only interested in the performance of the adaptive algorithm in beamforming, we assume a continuous signal is generated from the logistic map 1 as shown below:

$$g_{n+1} = 1 - 2g_n^2 \tag{7.13}$$

where the transmitted signal will be $s(t) = g_n$. The initial condition g_0 is randomly generated for each run.

Figures (7.9) and (7.10) show the MSE performance of the LMS, FWV-LMS and UWV-LMS beamforming for 2 antennas using a CSK transmitted signal

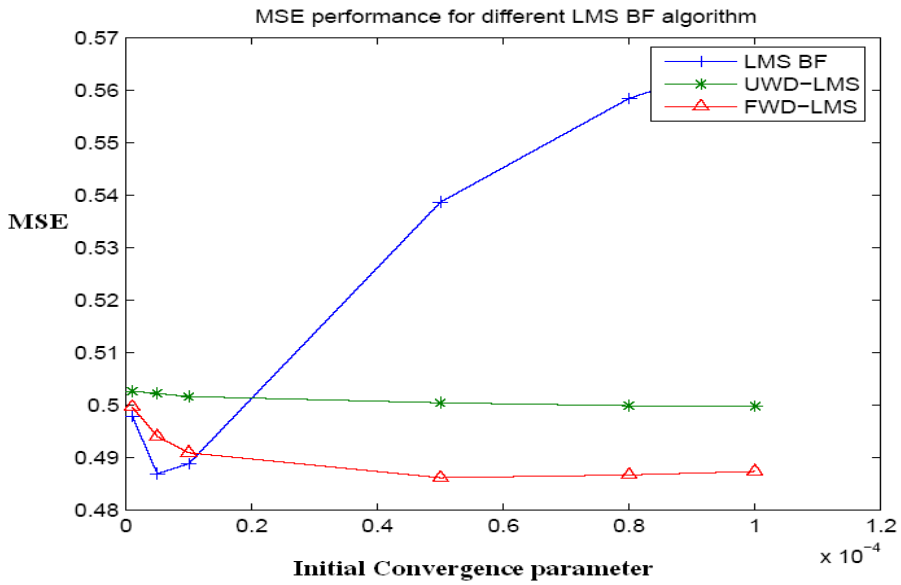

Figure 7.10: MSE performance of adaptive beamforming for CSK signal (2 antennas, SIR=[-10, -10], $\theta_i = [-30, 50]$, SNR = 10, $\alpha = 0.95$, $\delta = 0.00003$).

in a low SIR (-10 dB) environment. Figures (7.9) and (7.10) show that the WV-LMS algorithm still provide a better MMSE performance in general. The MMSE for both QFM and CSK signals are similar, hence, the proposed adaptive algorithm can be used for broadband CSK signals. Since the transmitted signal is now a broadband CSK signal, the algorithm will be more sensitive to the control parameters α and δ.

Figures (7.11) and (7.12) show the MSE performance of the LMS, FWV-LMS and UWV-LMS beamforming with 2 antennas using a CSK signal with a higher SIR (0dB) environment. The graphs show that under a higher SIR environment, the performance become very sensitive to the received signal. This behavior was not noticed when we used QFM signals. Hence, the algorithm may not be as suitable under high interference environment for CSK signals as for QFM signals.

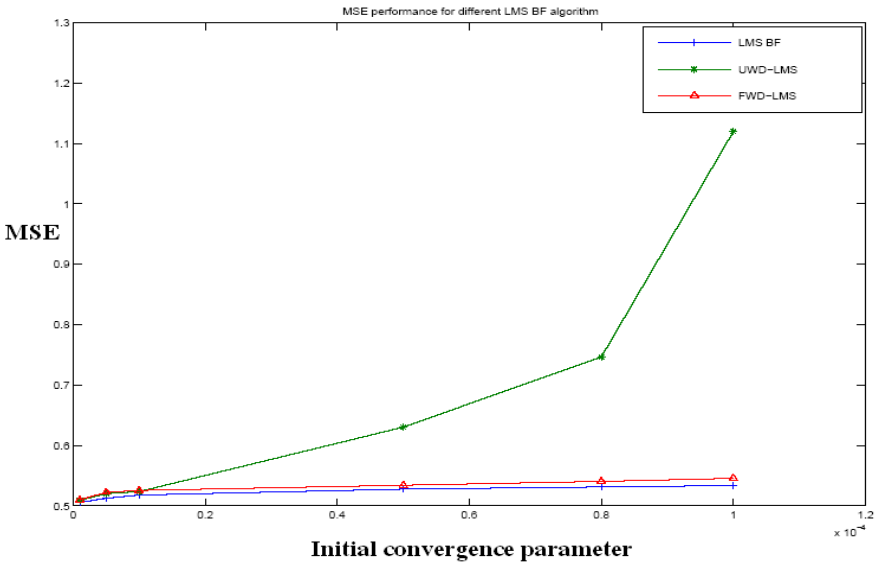

Figure 7.11: MSE performance for adaptive beamforming in CSK signal (2 antennas, SIR=[0, 0], $\theta_i = [-30, 50]$, SNR = 10, $\alpha = 0.90$, $\delta = 0.0005$).

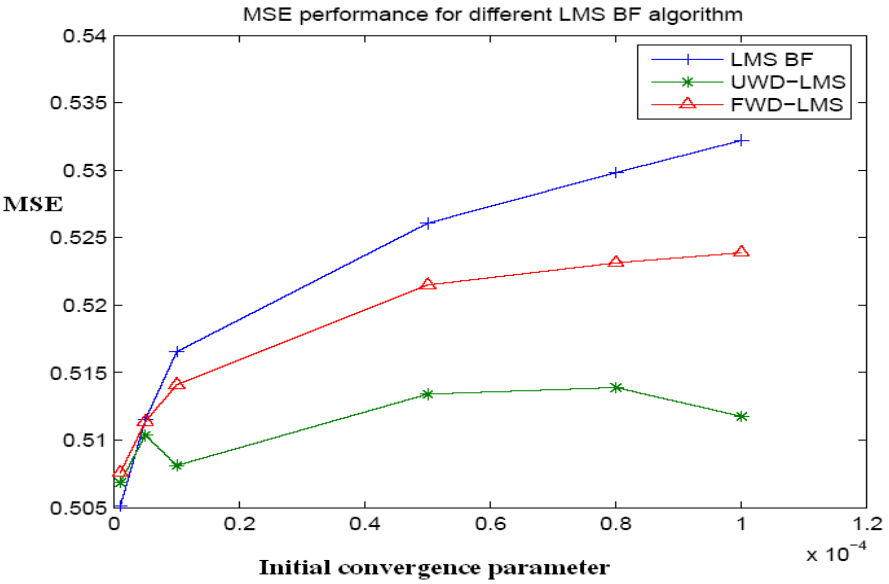

Figure 7.12: MSE performance for adaptive beamforming in CSK signal (2 antennas, SIR=[0, 0], $\theta_i = [-30, 50]$, SNR = 10, $\alpha = 0.9$, $\delta = 0.00003$).

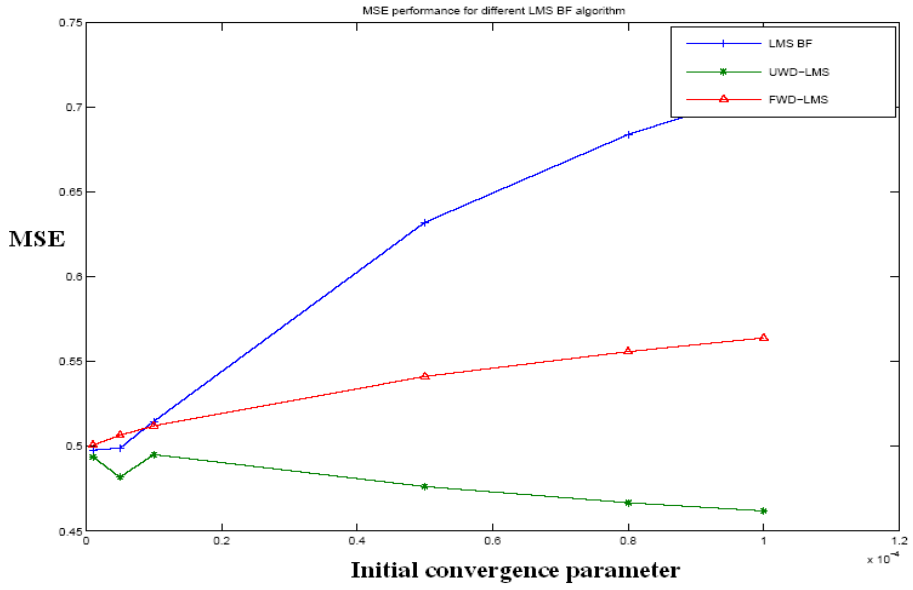

Figure 7.13: MSE performance for adaptive beamforming in CSK signal (4 antennas, SIR=[0, 0], $\theta_i = [-30, 50]$, SNR = 10, $\alpha = 0.90$, $\delta = 0.0005$).

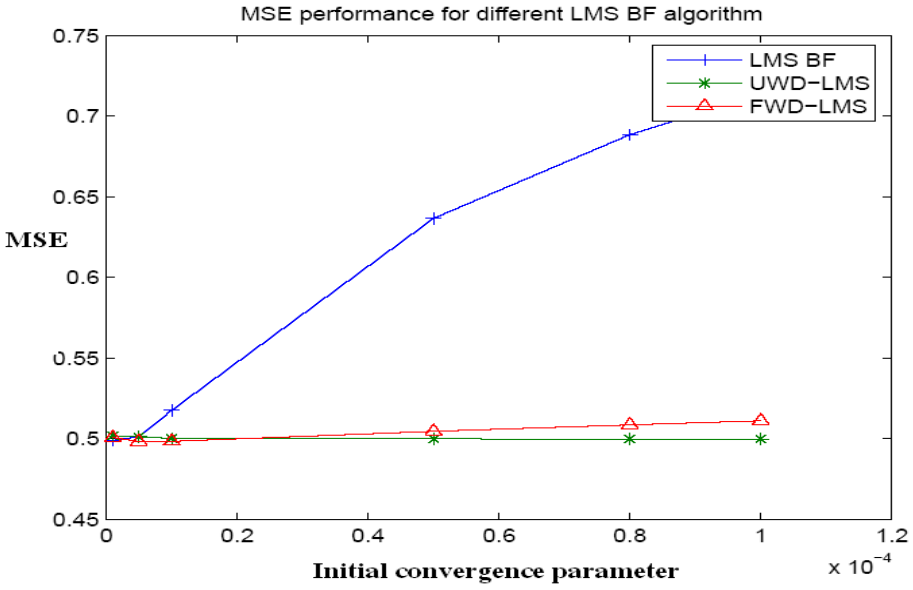

Figure 7.14: MSE performance for adaptive beamforming in CSK signal (4 antennas, SIR=[0, 0], $\theta_i = [-30, 50]$, SNR = 10, $\alpha = 0.9$, $\delta = 0.00003$).

Figures (7.13) and (7.14) show the MSE performance of the LMS, FWV-LMS and UWV-LMS beamforming with 4 antennas using a CSK signal with a higher SIR (0 dB) environment. Comparing 2 antennas to 4 antennas system in a high SIR environment, the 4 antennas system is not as sensitive to interference as the 2 antennas one, and it performs in an expected fashion. Hence, we should use higher number of antennas in a higher SIR environment. It is also clearly seen that the UWV-LMS algorithm outperforms the conventional LMS and FWV-LMS algorithms in terms of minimum MSE.

In general, figures (7.3- 7.14) show that the UWV-LMS has better performance when a larger initial convergence parameter μ_n is used. The parameters α and δ are used to control the WV-LMS algorithms performance and should be carefully selected. The algorithms can be used in beamforming for both narrow-band QFM and broadband CSK signal.

7.6 Conclusions

We presented two modifications to the conventional least mean-squared (LMS) algorithm using the forward prediction of the weights vector to dynamically modify the convergence parameter. The algorithms were tested in two different transmit signal types: quadratic FM (QFM) and chaos-shift-keying (CSK) signals. The study concentrated on the performance of the proposed algorithms in beamforming applications. In practical mobile communication systems, the physical size of the device is limited, and, as a result, only 2 and 4 antennas have been studied in our simulations.

The proposed algorithms, abbreviated as FWV-LMS and UWV-LMS, showed to provide better minimum mean-squared error (MMSE) than the conventional

LMS algorithm under different SIR conditions. The simulation results also showed that the performance of FWV-LMS is parallel to that of the conventional LMS algorithm, whereas the UWV-LMS is more adaptable depending on the predicted convergence parameter. Hence, we can have more control over the FWV-LMS algorithm than the UWV-LMS algorithm. However, UWV-LMS will perform better under a dynamic channel environment. Generally, the algorithm provides similar MSE performance for both CSK and QFM signals. Further study is needed to understand this performance in other channel environments (models) and to extend the algorithm dynamic range for CSK signals.

Chapter 8

Adaptive Algorithms for Performance Enhancement in Chaos Communication

8.1 Introduction

The primary feature of an adaptive algorithm is the ability to self-adjust its coefficients according to the system conditions. Accordingly, adaptive algorithms can be applied under many signal conditions such as linear and nonlinear signal environments [72]. Adaptive algorithms have been extensively studied in the past few decades and have been widely used in many arenas including biomedical, image and speech processing, communication signal processing and many other applications [71, 72, 114].

In the communications industry, there are a lot of works that utilize the LMS and RLS algorithms for channel estimation, equalization, and demodulation [40, 115, 116]. The performance of these adaptive algorithms is highly dependent on their filter order and the signal condition. Furthermore, the performance of the LMS algorithm also depends on the selected convergence parameter μ. As for the RLS algorithm, it is also dependent on a parameter λ commonly known

as "forgetting factor" or "exponential weighting factor" [114]. In this Chapter we will only consider the version of RLS named as the "growing window" RLS algorithm (with $\lambda = 1$) [114].

A new version of the LMS algorithm with time-varying convergence parameter is proposed in this chapter. The time-varying LMS (TV-LMS) algorithm utilizes a time-varying convergence parameter μ_n (n being the sample count) with a time-decaying law. The basic idea behind this structure is the fact that the conventional LMS algorithm needs a relatively large value for the convergence parameter μ if we want to speed up the convergence of the filter coefficients to their optimal values, but a lower value for μ if we want more accurate estimation (less mean-squared error, MSE). We expect better performance if μ is adjusted to be time-dependent with a decaying law such that it has a large value at the beginning to ensure faster convergence of the coefficients to their optimal values, then, as time passes, the convergence parameter takes on smaller values for better estimation accuracy [114]. The parameter μ should reach a steady state whose value is application dependent. A general power decaying law has been proposed; however, other time-varying laws could also be applicable.

In this chapter we concentrate on noise reduction as a primary function of adaptive algorithms to compare their performance. We present a study of the conventional LMS algorithm, the proposed TV-LMS algorithm, and the RLS algorithm in terms of their execution time, filter order, mean-squared error (MSE) performance, and speed of convergence. Initially, We use MATLAB simulation to study the properties of the algorithm for a single-tone linear signal. Then, We carry it on to examine the behavior of this algorithm for non-linear FM signals. Finally, we evaluate the performance of these algorithms for a real chaos communication signal in the presence of additive white Gaussian noise

(AWGN).

8.2 Selected Adaptive Algorithms

In this section we present a brief description of the conventional LMS and RLS algorithms and propose the time-varying LMS algorithm.

8.2.1 The Conventional LMS Algorithm

In the conventional adaptive LMS algorithm, the weight vector coefficients $\mathbf{w}(n)$ for the FIR filter are updated according to the formula [71, 72, 114, 115, 116]:

$$\mathbf{w}(n) = \mathbf{w}(n-1) + \mu e(n)\mathbf{y}(n) \tag{8.1}$$

where $\mathbf{w}(n) = [w_o(n) \;\; w_1(n)...w_M(n)]$ ($M+1$ being the filter length), μ is the convergence parameter (sometimes referred to as *step-size*), $e(n) = d(n) - z(n)$ is the output error ($z(n)$ being the filter output), and $d(n)$ is the reference signal. Note that $z(n) = \mathbf{w}(n-1)\mathbf{y}^T(n) = \hat{x}(n)$, where $\hat{x}(n)$ is the original signal and $\mathbf{y}(n) = [y(n) \;\; y(n-1)...y(n-M)]$ is the input signal to the filter.

8.2.2 A Time-Varying LMS Algorithm

Abbreviated as TV-LMS algorithm; it works in the same manner as the conventional LMS algorithm, except for a time-dependent convergence factor μ_n. The time-varying law depends on the kind of signals and their expected range of frequencies, hence it is application - dependent. We will consider single-tone sinusoids, linear and non-linear narrowband FM signals, then proceed to chaotic signals. For single-tone sinusoids, there is an optimal value for the con-

vergence parameter μ that gives minimum MSE. This value of μ is frequency dependent, as we will see in Section 8.3. If a sinusoidal input is expected with a frequency in the range $[f_1, f_2]$, then the practical choice of the steady-state value of the convergence parameter μ_o is that which corresponds to the frequency $f_o = (f_1 + f_2)/2$. For narrowband FM signals, we must first define the optimal μ_o for the center frequency or the mean frequency f_m. To do so, the conventional LMS algorithm is used (with a single-tone of frequency f_m) to find the optimal value of μ at that frequency. This optimal value μ_o is used to update the time-varying convergence parameter μ_n according to the following formula:

$$\mu_n = \alpha_n \times \mu_o \tag{8.2}$$

where α_n is a decaying factor. We will consider the following decaying law:

$$\alpha_n = C^{\frac{1}{1+an^b}} \tag{8.3}$$

where C, a, b are positive constants that determine the magnitude and the rate of decrease for α_n. According to the above law, C has to be a positive number larger than 1. When $C = 1$, α_n will be equal to 1 and the new algorithm will be the same as the conventional LMS algorithm. An outline of the TV-LMS algorithm is shown in the following steps :

$$z(n) = \mathbf{w}(n-1)\mathbf{y}^T(n) \tag{8.4}$$

$$e(n) = d(n) - z(n) \tag{8.5}$$

$$\alpha_n = C^{\frac{1}{1+an^b}} \tag{8.6}$$

$$\mu_n = \alpha_n \times \mu_o \tag{8.7}$$

$$\mathbf{w}(n) = \mathbf{w}(n-1) + \mu_n e(n)\mathbf{y}(n) \tag{8.8}$$

where ^{T} indicates matrix transposition.

8.2.3 The Conventional RLS Algorithm

As compared to the LMS algorithm, the RLS algorithm has the advantage of fast convergence, but this comes at the cost of increasing the complexity. The RLS algorithm consumes longer computation time and has a higher sensitivity to numerical instability than the LMS algorithm [71, 40, 114]. In this paper, we consider the RLS algorithm in the following form [71, 114, 116]:

$$z(n) = \mathbf{w}(n-1)\mathbf{y}^T(n) \tag{8.9}$$

$$e(n) = d(n) - z(n) \tag{8.10}$$

$$\mathbf{k}(n) = \frac{\mathbf{P}(n-1)z(n)}{\lambda + z^H(n)\mathbf{P}(n-1)z(n)} \tag{8.11}$$

$$\mathbf{P}(n) = \frac{\mathbf{P}(n-1) - \mathbf{P}(n-1)z^H(n)\mathbf{k}(n)}{\lambda} \tag{8.12}$$

$$\mathbf{w}(n) = \mathbf{w}(n-1) + e(n)\mathbf{k}(n) \tag{8.13}$$

where ^{H} indicates the Hermitian property.

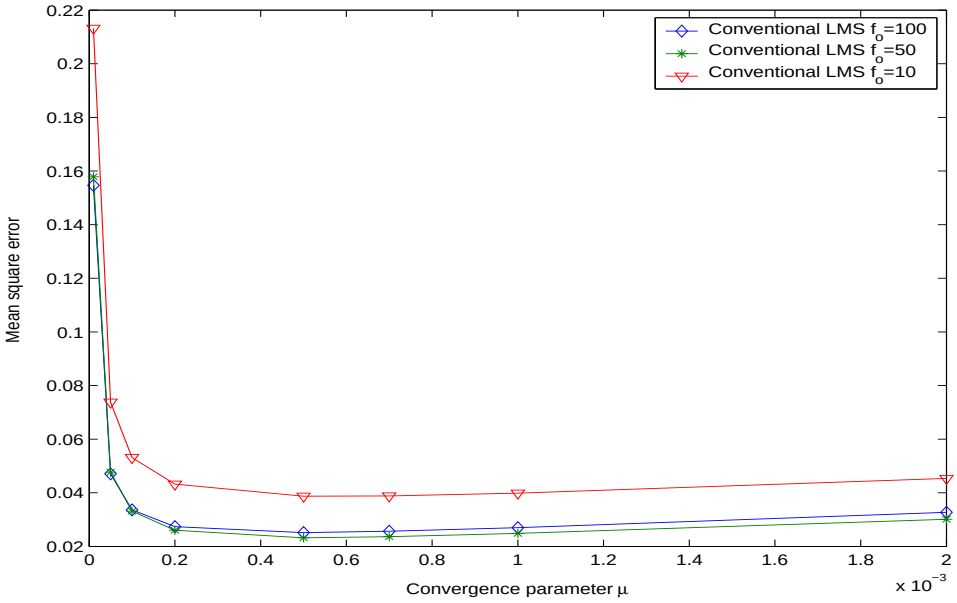

Figure 8.1: MSE performance for the conventional LMS with different μ and different input frequencies f_o (SNR = 2 dB).

8.3 Performance Results

In this section we present MATLAB simulation of the above adaptive algorithms. The input signal for all algorithms has the form $\mathbf{y}(t) = \mathbf{x}(t) + \mathbf{n}(t)$, $\mathbf{n}(t)$ being white Gaussian noise with 2 dBW power and $\mathbf{x}(t)$ is the original signal. To begin with, a single-tone sinusoid signal is used as the original signal $\mathbf{x}(t)$. This signal is of fundamental importance for the time-varying approach. A quadratic frequency-modulated (QFM) signal is then used to study the algorithms' performance under nonlinear narrow-band signal conditions. At last the algorithm is applied to chaos shift-keying (CSK) signals.

8.3.1 Single-Tone Sinusoids

We first consider a single-tone signal $A\sin(2\pi f_o t)$.

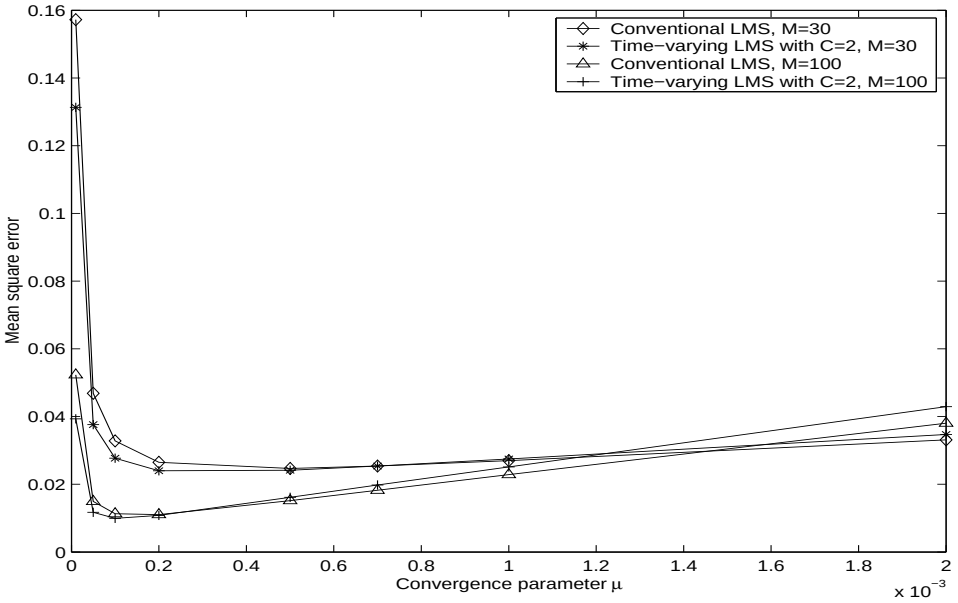

Figure 8.2: MSE performance for the LMS and TV-LMS algorithms with different μ_o (SNR = 2 dB, single-tone at $f_o = 100$ Hz).

Figure (8.1) shows the MSE performance of the conventional LMS algorithm with difference values of μ and different input frequencies. The mean squared error (MSE) for each convergence parameter is calculated as follows:

$$MSE = \frac{1}{N}\sum_{n=0}^{N}[x(n) - \hat{x}(n)]^2 \tag{8.14}$$

where $x(n)$ is the original signal and $\hat{x}(n)$ is the filter output, which represents an estimate of the input signal. Figure (8.1) shows that the performance for the conventional LMS algorithm is frequency dependent, with an optimal value of μ for each frequency. Hence, the choice of the optimal μ is application - dependent.

Figures (8.2) and (8.3) show the MSE performance of the TV-LMS and the conventional LMS algorithms with different values of μ and different filter

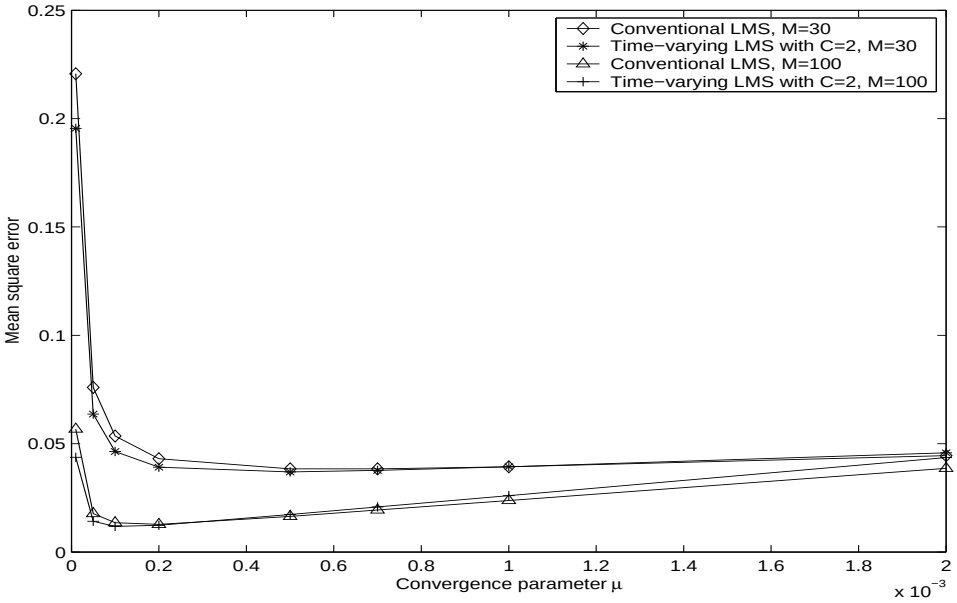

Figure 8.3: MSE performance for the LMS and TV-LMS algorithms with different μ_o (SNR = 2 dB, single-tone at $f_o = 10$ Hz).

orders. These figures show that both algorithms provide similar performance results. Their optimal μ_o is sitting at smaller μ region ($< 0.4 \times 10^{-3}$) and the performance is better when the filter order is larger. The results show that, for both TV-LMS and conventional LMS algorithms, a higher filter order should be used in order to provide a better MSE performance for the system. Comparing the filter order used in figure (8.2) with that in figure (8.3), it is clear that the optimal μ_o is dependent on the filter order as well as the frequency. The higher the filter order the smaller the optimal μ_o will be. The overall performance of the TV-LMS algorithm is better than that of the conventional LMS algorithm.

Figures (8.4) and (8.5) show the MSE performance of the TV-LMS algorithm and conventional LMS algorithm with different filter orders and different values of the parameter C. Again, both LMS algorithms provide similar performance results. The larger the parameter C the less the MSE. It is clear that the TV-

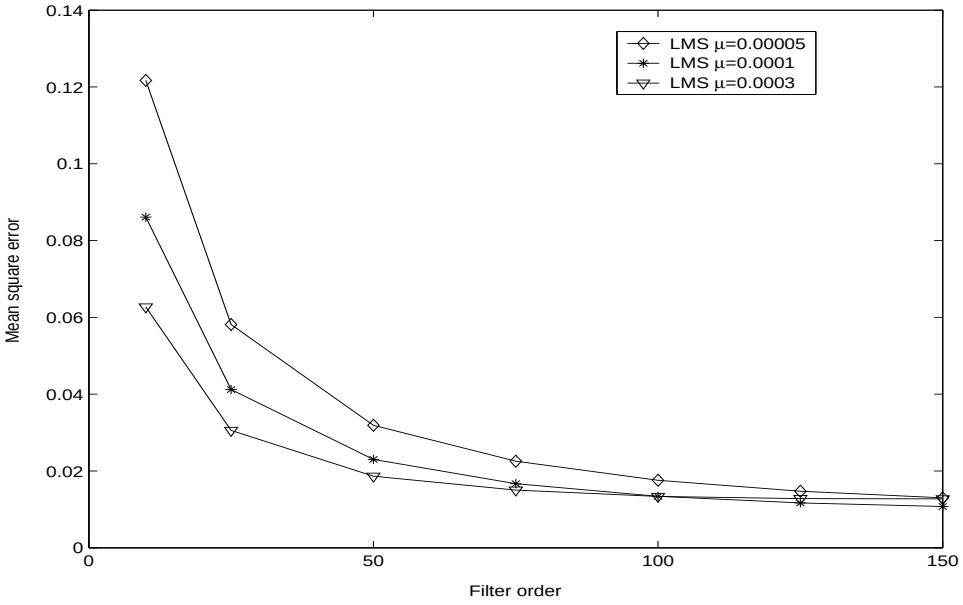

Figure 8.4: MSE performance of the LMS algorithm with different filter orders (SNR = 2 dB, single-tone at $f_o = 100$ Hz).

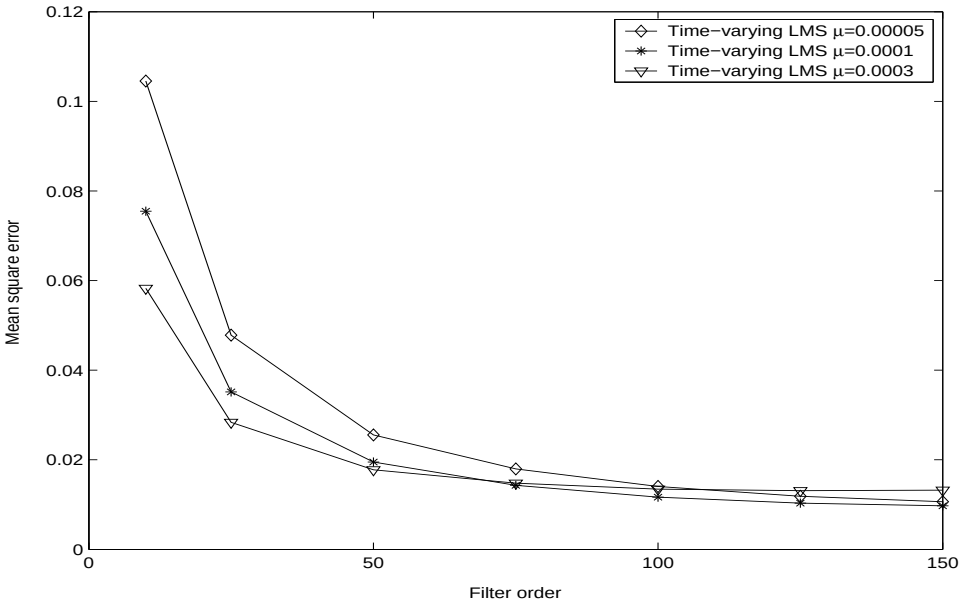

Figure 8.5: MSE for the time-varying LMS (TV-LMS) algorithm with different filter orders (SNR = 2 dB, single-tone at $f_o = 100$ Hz, $C = 2, a = 0.01, b = 0.7$).

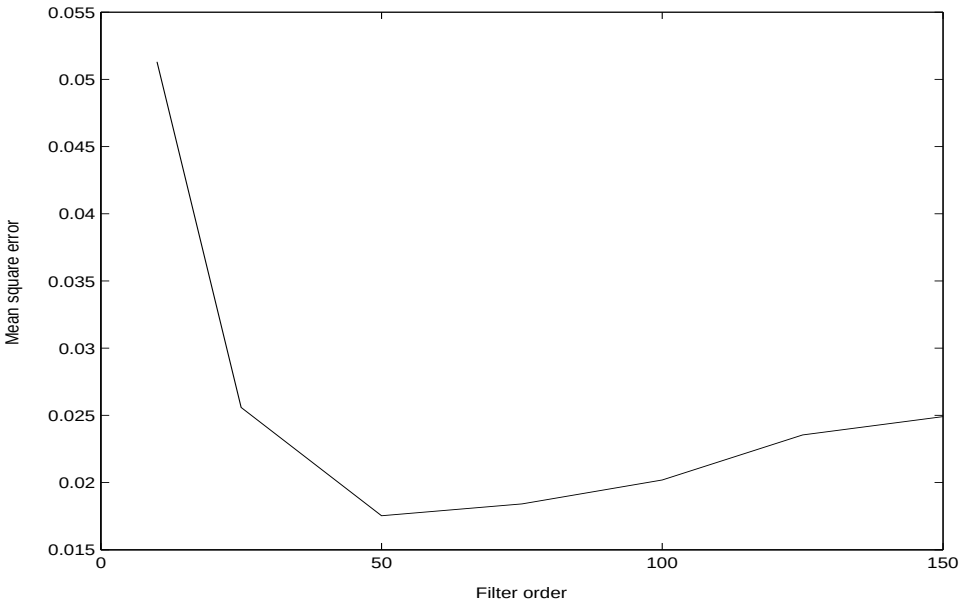

Figure 8.6: MSE for the RLS algorithm with different filter orders (SNR = 2 dB, single-tone at $f_o = 100$ Hz, $\lambda = 1$).

LMS algorithm performs much better than the conventional LMS algorithm in the low filter order region. Figures (8.4) and (8.5) also show that both algorithms provide better MSE performance when the filter order increases.

Figure (8.6) shows the MSE performance for the RLS ($\lambda = 1$) algorithm with different filter orders. As the RLS is highly sensitive to numerical instability [71, 40, 114], the filter order will severely affect the performance of the algorithm. Figure (8.6) shows that there is no improvement in the performance of the RLS algorithm when the filter order increases. Its optimal filter order in this case is around 50. A careful selection of the filter order is therefore needed for optimal performance.

Figures (8.7) and (8.8) show the mean-squared error versus the number of samples N for different algorithms. These figures provide information about the adaptive filter convergence time. It can be noticed that the RLS provides

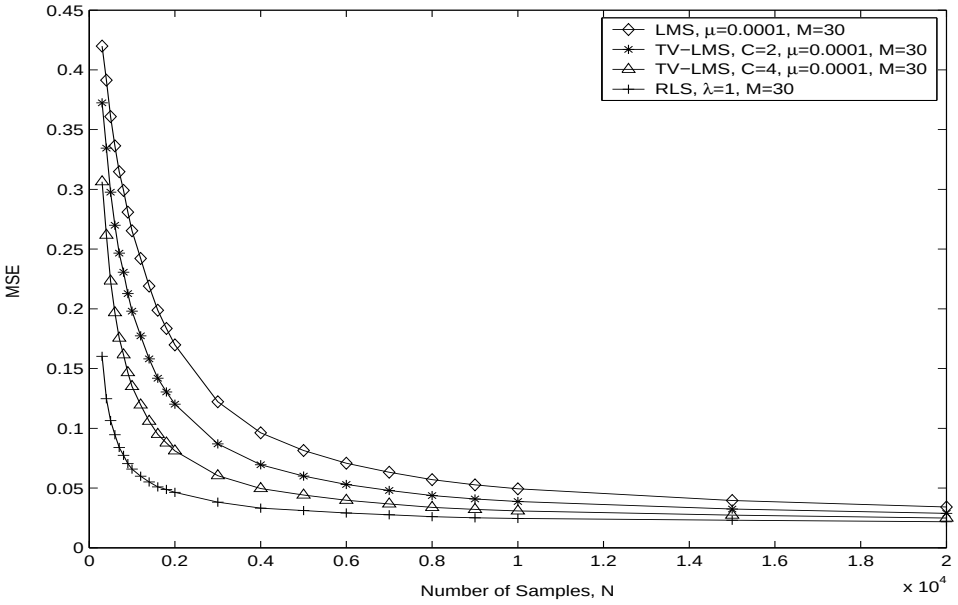

Figure 8.7: MSE vs. number of samples for different adaptive algorithms (SNR = 2 dB, $M = 30$, $f_o = 100$ Hz).

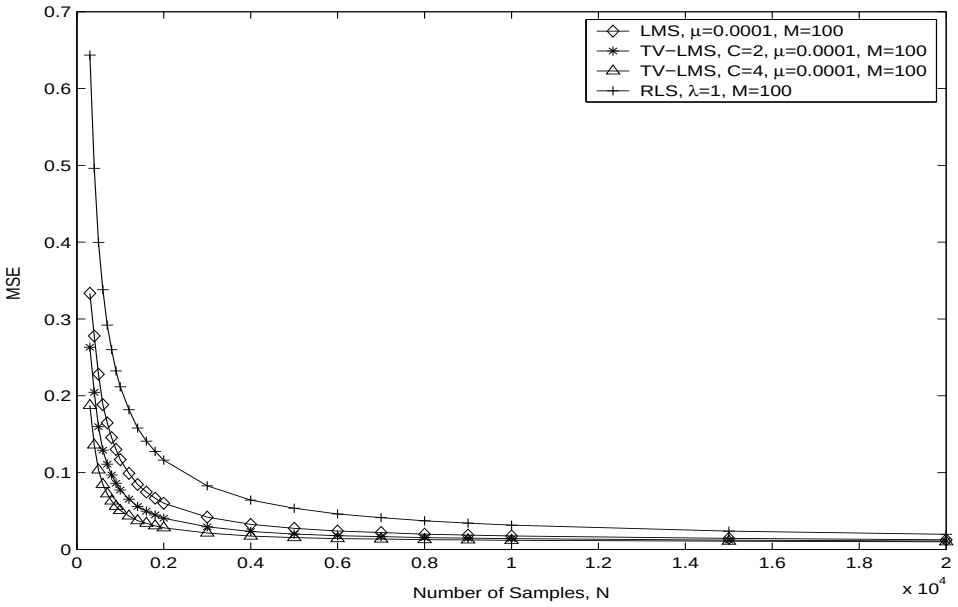

Figure 8.8: MSE vs. number of samples for different adaptive algorithms (SNR = 2 dB, $M = 100$, $f_o = 100$ Hz).

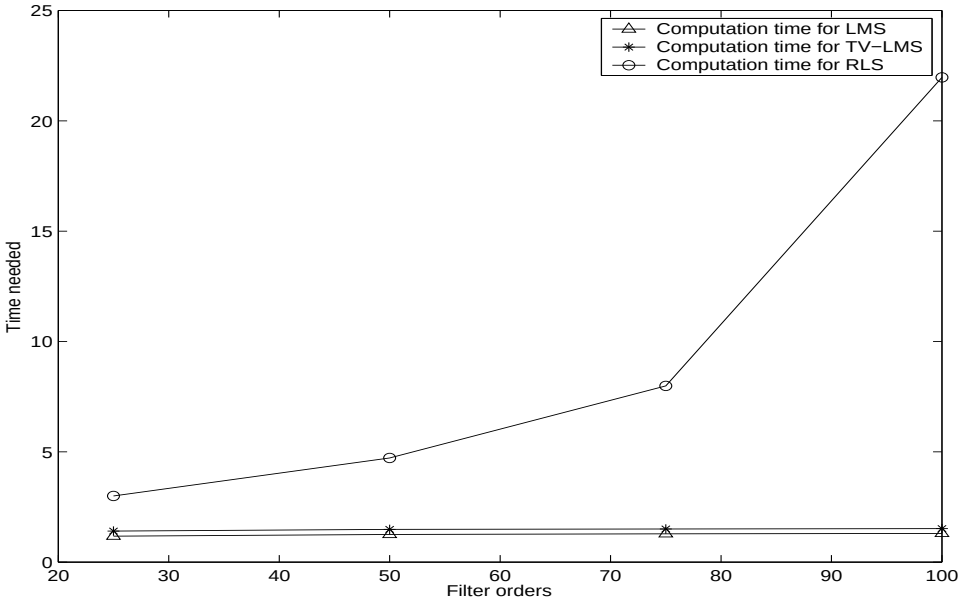

Figure 8.9: Computation time of different adaptive algorithms with different filter orders.

fastest convergence time; it also gives the best MSE performance when filter order is small. However, this comes at the cost of computation time needed for RLS as shown in figure (8.9).

Figure (8.9) shows the computational time for different algorithms with different filter orders. The computation time for the conventional LMS algorithm and the TV-LMS algorithm is relatively similar and much less than that of the RLS algorithm. The above figures also show that the RLS computation time increases rapidly and non-linearly with the filter order.

8.3.2 Quadratic Frequency-Modulated (QFM) Signals

As non-linear FM signals are important in application (such as communication signal, biomedical signal and etc), we assume here that the original signal $\mathbf{x}(t)$

is a finite-length QFM signal as follows:

$$x(t) = \sin(\omega_o t + \alpha t^2/2 + \beta t^3/3)\Pi_T(t - T) \tag{8.15}$$

where $\omega_o = 2\pi f_o$ is a constant (initial frequency), T is the signal duration, $\Pi_T(t)$ is the rectangular box function, and α and β are the modulation indices which determine the bandwidth of the QFM signal.

The bandwidth BW of this QFM signal can be adjusted by varying the parameters α and β, as can be numerically shown using the relationships [113]:

$$f_m = \frac{1}{2\pi}\frac{\int_0^\infty \omega|X(\omega)|^2 d\omega}{\int_0^\infty |X(\omega)|^2 d\omega} \tag{8.16}$$

$$BW = \frac{1}{2\pi}\int_0^\infty (\omega - \omega_m)^2|X(\omega)|^2 d\omega \tag{8.17}$$

where $X(f)$ is the Fourier transform of $x(t)$ and f_m is its mean frequency.

Figures (8.10) and (8.11) show the mean-squared error (MSE) performance of the conventional LMS algorithm and the time-varying LMS (TV-LMS) algorithm using different filter orders and different QFM bandwidths. Again, results show that the TV-LMS algorithm performs better than LMS algorithm, which is similar to result shown in the previous section for noise reduction in single-tones (Figure 8.2). Comparing the bandwidths in figures (8.10) and (8.11), the performance for both algorithms decreases slightly when the QFM signal bandwidth increases. The results are still in an acceptable range, therefore, the algorithm can be used for narrowband signals with similar performance curves. Figures (8.10) and (8.11) also indicate that increasing the filter order does not provide much improvement in the MSE performance.

Figures (8.12) and (8.13) show the MSE performance of the conventional

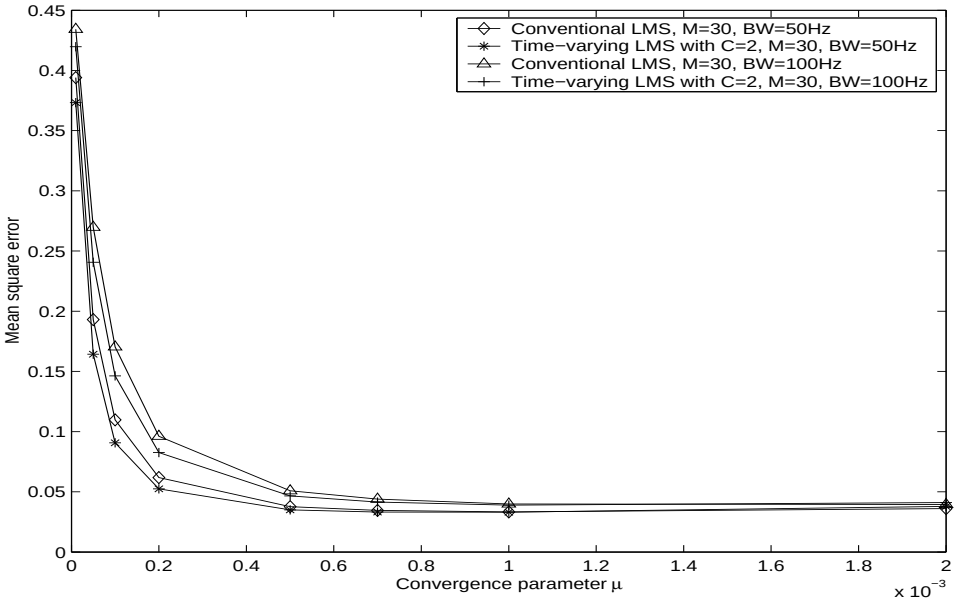

Figure 8.10: MSE performance for the LMS and TV-LMS algorithms with different μ_o, filter order $M = 30$, and different bandwidths (SNR = 2 dB, $f_o = 100$ Hz).

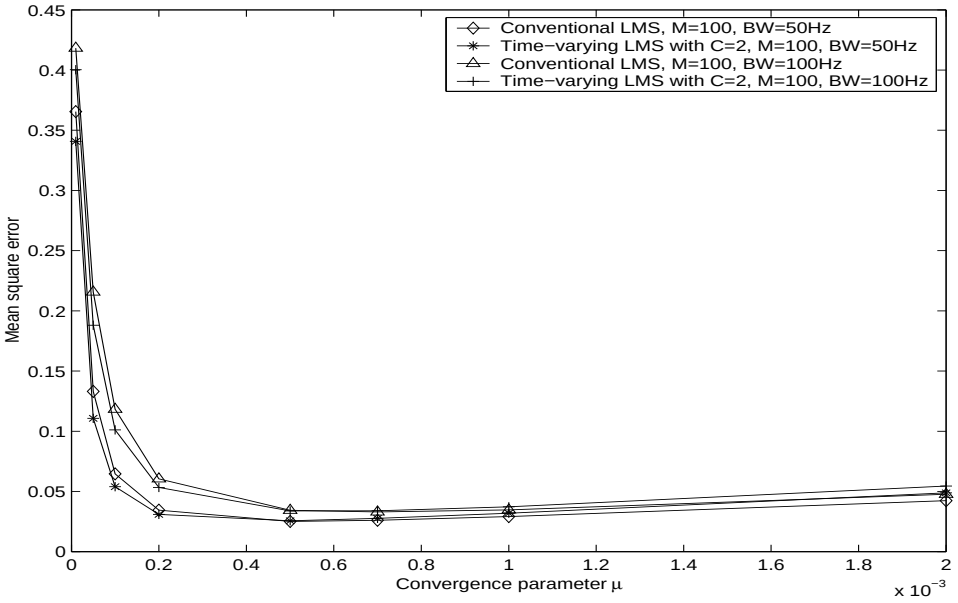

Figure 8.11: MSE performance for the LMS and TV-LMS algorithms with different μ_o, filter order $M = 100$, and different bandwidths (SNR = 2 dB, $f_o = 100$ Hz).

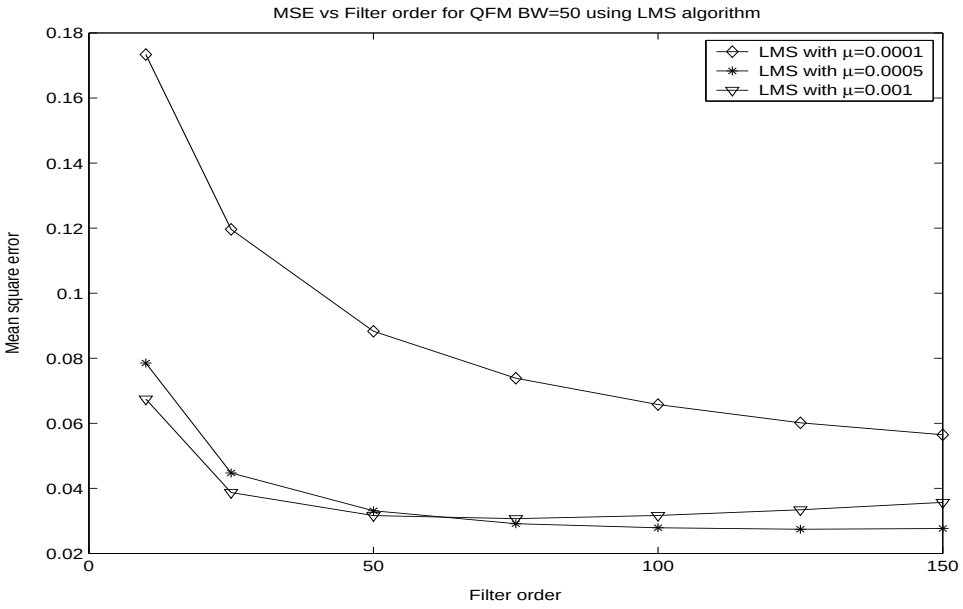

Figure 8.12: MSE for the LMS algorithm with different filter orders in QFM signal BW = 50 Hz (SNR = 2 dB, $a = 0.01, b = 0.7$).

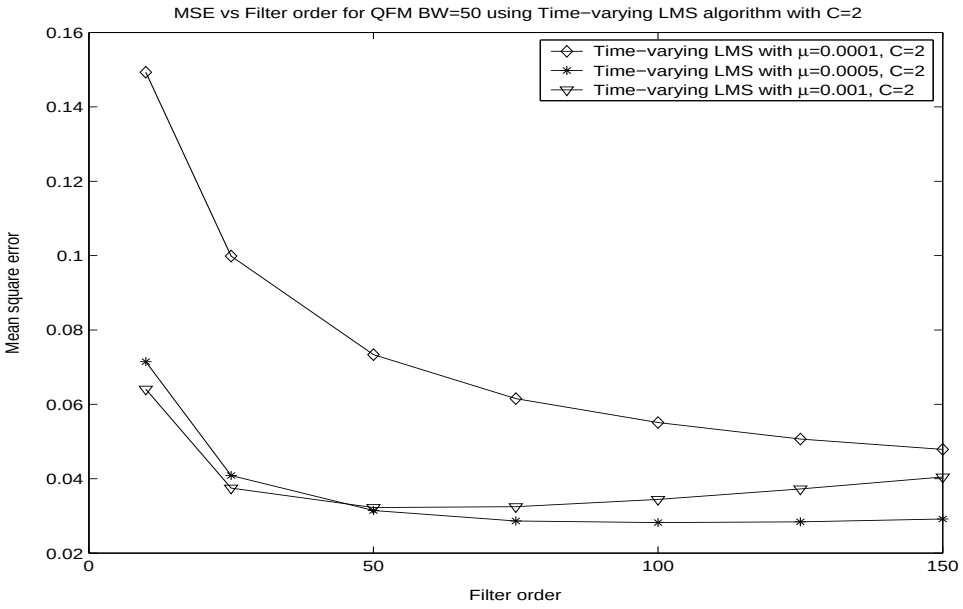

Figure 8.13: MSE for the TV-LMS algorithm with different filter orders in QFM signal BW=50 Hz (SNR = 2 dB, $C = 2, a = 0.01, b = 0.7$).

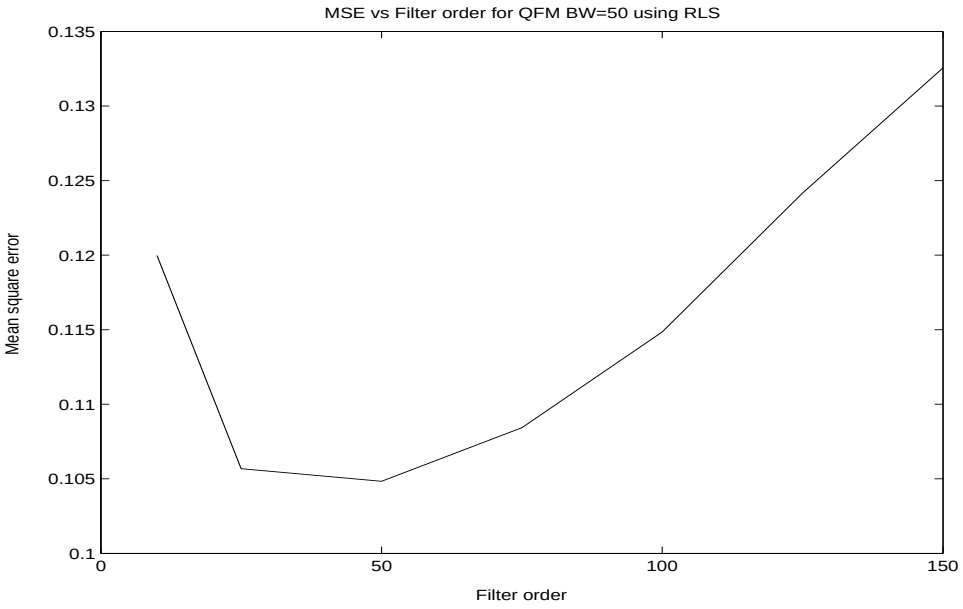

Figure 8.14: MSE for the RLS algorithm with different filter orders for QFM signal with $BW = 50$ Hz (SNR = 2 dB, $a = 0.01, b = 0.7$).

LMS algorithm and the TV-LMS algorithm with different filter orders and different values of the C parameter. In general, results show that the performance will improve when the filter order increases. However, this is not true for μ values that are too far from the optimal range. Figures (8.12) and (8.13) also show that TV-LMS performs better with larger C. Again, this is in accord with Figures (8.4) and (8.5).

Figure (8.14) shows the MSE performance for the RLS ($\lambda = 1$) algorithm with different filter orders. Figure (8.14) provides an identical conclusion for the RLS algorithm as in figure (8.6); RLS shows no improvement when the filter order increases. Compared with figures (8.12) and (8.13), Figure (8.14) also shows that the RLS algorithm performs worse than conventional LMS algorithm and the time-varying LMS algorithm in this nonlinear QFM environment. It can be concluded that the TV-LMS algorithm provides a computation time close

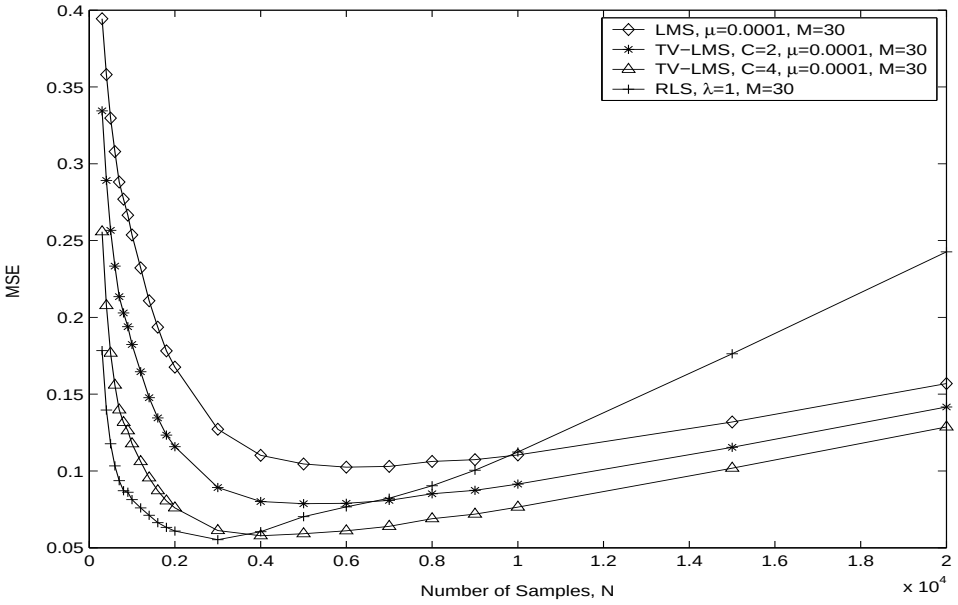

Figure 8.15: MSE vs. number of samples for different adaptive algorithms (SNR = 2 dB, $M = 30$).

to that of the conventional LMS algorithm, with the best MSE performance in QFM signal environments.

Figures (8.15) and (8.16) show the mean-squared error versus the number of samples N. In figure (8.15), the RLS algorithm can provide a fast converging speed. However, it starts to fall apart and its MSE performance worsens as time passes. Hence, the RLS does not provide the same benefits for QFM signal as it did for a single-tone sinusoid (figures 8.7 and 8.8). In general, it is shown that the TV-LMS algorithm has faster convergence than the LMS for both single-tone sinusoid (figures 8.7 and 8.8) and QFM signal (figures 8.15 and 8.16).

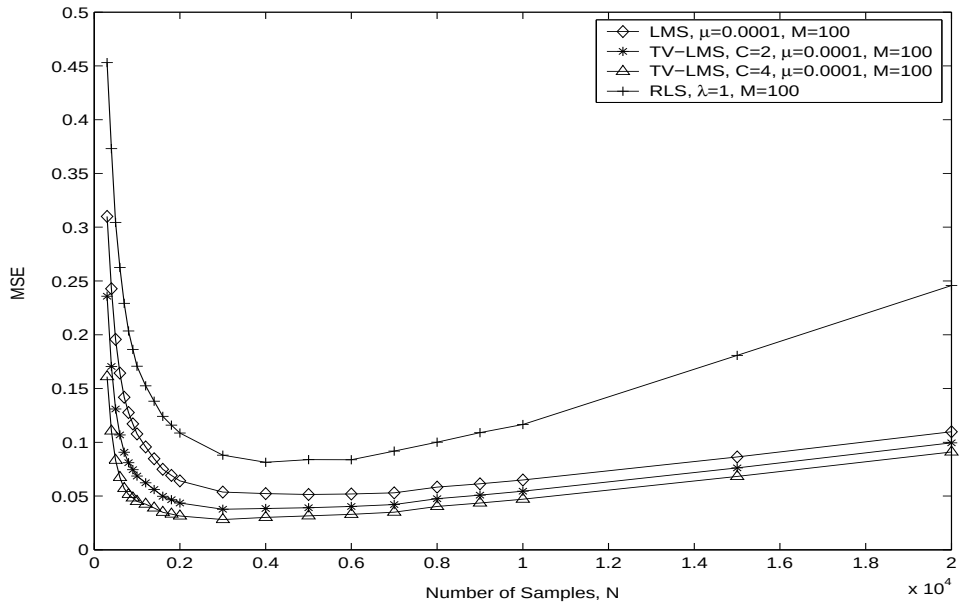

Figure 8.16: MSE vs. number of samples for different adaptive algorithms (SNR = 2 dB, $M = 100$).

8.3.3 Chaos Shift-Keying (CSK) Signals

Here we study the effect of adaptive noise reduction algorithms for chaos communication signals. The CSK signal $\mathbf{x}(t)$ is a finite-length transmitted LCG1 CSK signal that has been explained in previous chapters:

$$x(t) = 1 - 2(x(t-1))^2. \tag{8.18}$$

Figure (8.17) shows the mean-squared error (MSE) performance of the conventional LMS and the time-varying LMS (TV-LMS) algorithms with different filter orders and different values of μ for a chaos signal. The figure shows that TV-LMS provide better performance in terms of reducing the MSE under a non-linear signal environment. The optimal μ_o is sitting at even smaller μ region and is even more smaller than those for single-tone and QFM signals. The

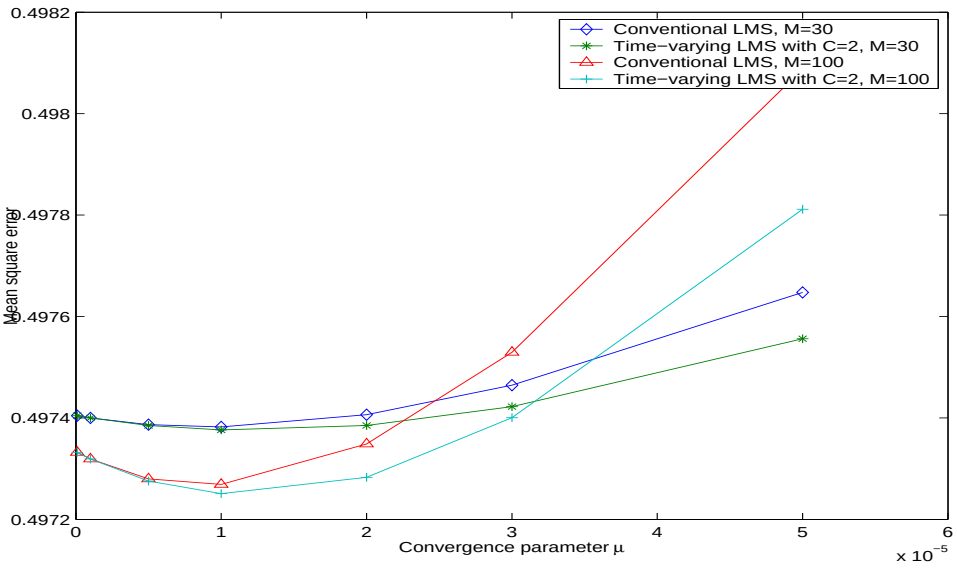

Figure 8.17: MSE performance for the LMS and TV-LMS algorithms for CSK with different μ_o, filter order $M = 30$ and $M = 100$, SNR = 2 dB.

results show that for both TV-LMS and conventional LMS algorithms, a higher filter order can potentially provide a better MSE performance for the system. In the next few figures, we will show that a higher order for the filter may not be as good for this non-linear dynamical signal. It is worth noticing that the optimal performance is directly dependent on the choice of optimal μ_o and the filter order. A careful selection is highly needed when applying the algorithms under a non-linear CSK signal environment. In general, the overall performance of the TV-LMS algorithm is better than that of the conventional LMS algorithm.

Figures (8.18) and (8.19) show the MSE performance of the conventional LMS and the TV-LMS algorithms with different filter orders. The results again confirm that there is no benefit in increasing the filter order under non-linear signal environments, where convergence of performance is seen at a filter order of 50 and above. In the case of non-linear wideband CSK signal, an optimal filter

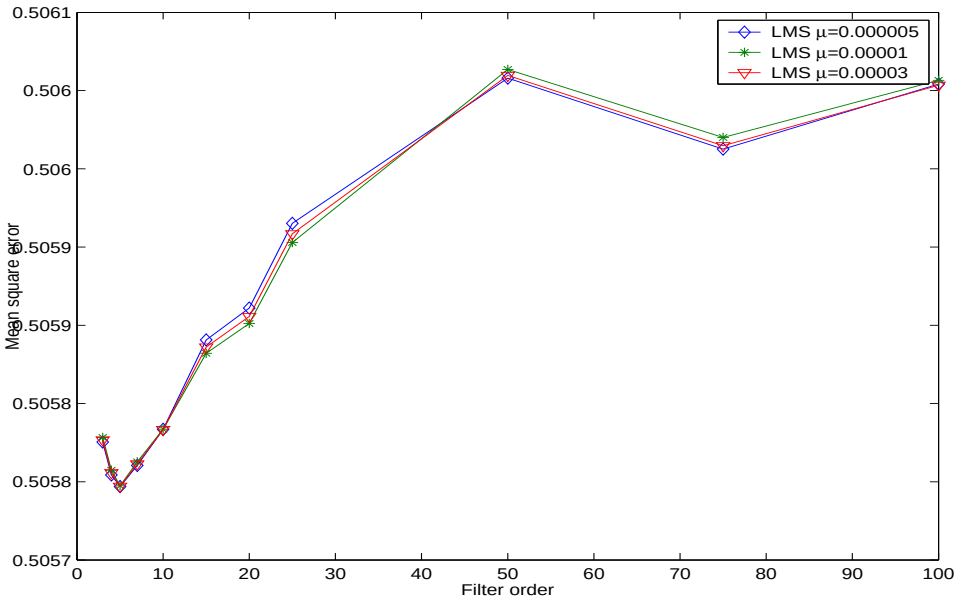

Figure 8.18: MSE for the LMS algorithm with different filter orders for CSK signal (SNR = 2 dB, $a = 0.01, b = 0.7$).

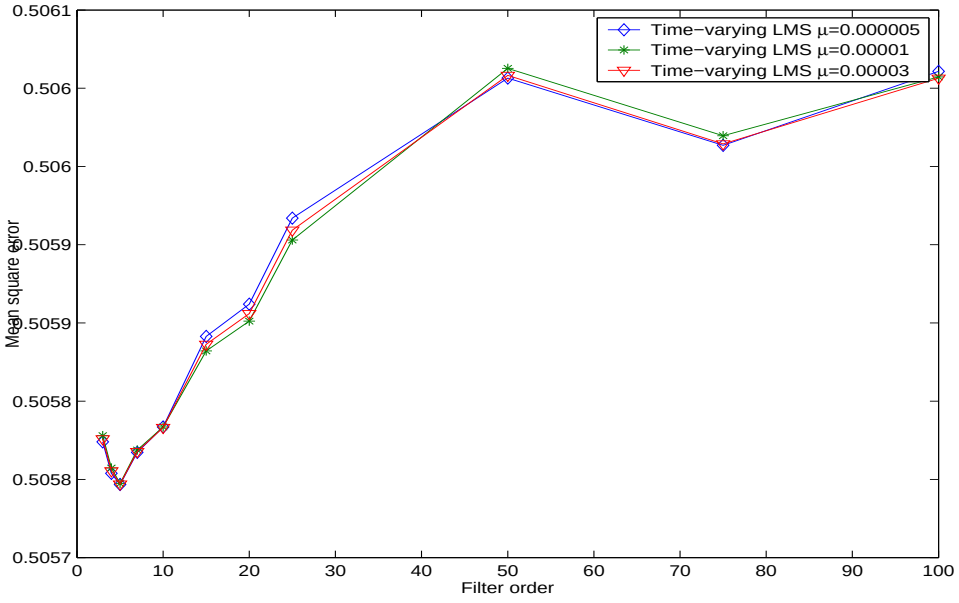

Figure 8.19: MSE for the TV-LMS algorithm with different filter orders for CSK signal (C = 2, SNR = 2 dB, $a = 0.01, b = 0.7$).

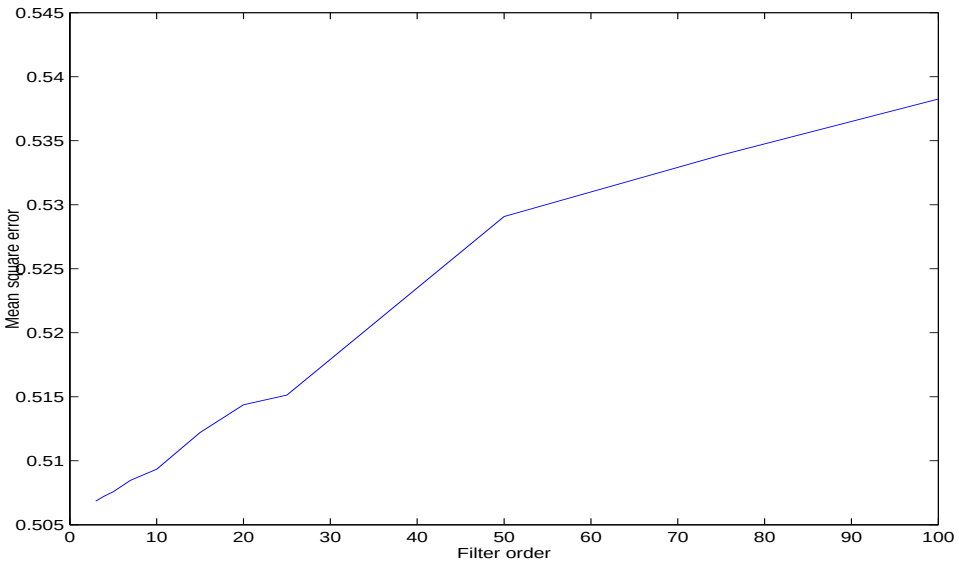

Figure 8.20: MSE for the RLS algorithm with different filter orders for CSK signal (C = 2, SNR = 2 dB, $a = 0.01, b = 0.7$).

order for both LMS and TV-LMS algorithms is around 5. It is also noted that there is no significant performance difference between the LMS and TV-LMS for non-linear wideband CSK signals.

Figure (8.20) shows the MSE performance of the RLS ($\lambda = 1$) algorithm with different filter orders. Since, RLS is sensitive to number instability, RLS shows no improvement when the filter order increases in this case.

Figures (8.21) and (8.22) show the mean-squared error versus the number of samples N. These graphs give an idea of the convergence speed for the adaptive algorithms. In a previous section, we saw that the RLS algorithm can provide a fast convergence under single-tone sinusoids. However, in the CSK case, both LMS and TV-LMS converge at a faster rate. We recall that the TV-LMS algorithm does not provide faster convergence than the LMS for both single-tone sinusoid (figures 8.7,8.8) and QFM signal (figures 8.15, 8.16).

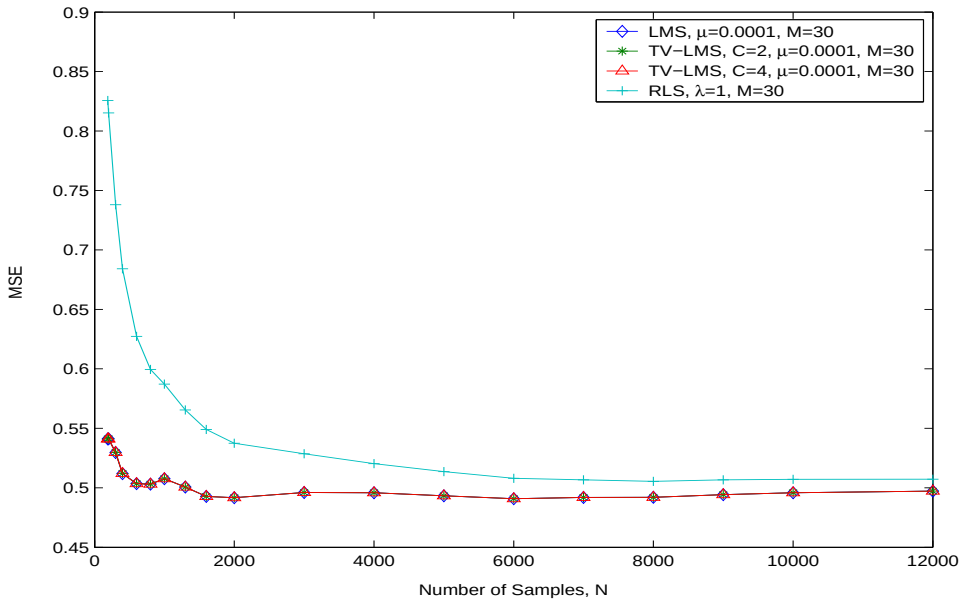

Figure 8.21: MSE vs. number of samples for different adaptive algorithms with CSK signal (SNR = 2 dB, $M = 30$).

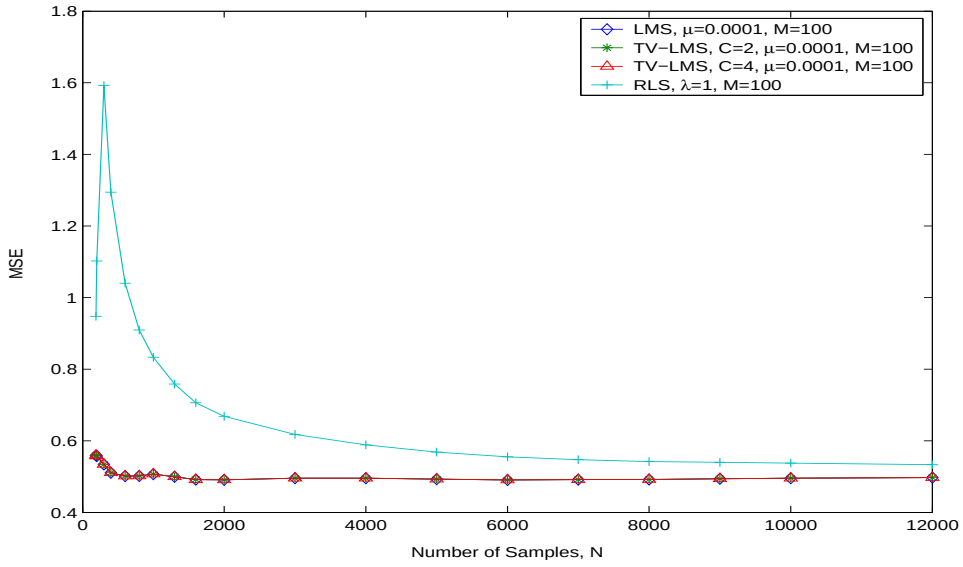

Figure 8.22: MSE vs. number of samples for different adaptive algorithms with CSK signal (SNR = 2 dB, $M = 100$).

8.4 Conclusion

In this chapter we proposed a time-varying LMS (TV-LMS) algorithm and presented a comprehensive study of its performance as compared to other well-known algorithms: the conventional LMS algorithm and the recursive least-squared (RLS) algorithm. The study concentrated selected noise reduction in single-tone sinusoids, non-linear quadratic FM signals and secure chaos communication signals. Four performance criteria are used in this comparison: the algorithm execution time, the minimum mean-squared error (MSE), the filter order, and the algorithm convergence speed. The TV-LMS algorithm with a decaying time-varying law for the convergence parameter was shown to have better performance than the conventional LMS algorithm in terms of faster convergence and less mean squared error.

For noise reduction in a single-tone sinusoid with additive white Gaussian noise (AWGN), larger filter order will provide better MSE performance for both conventional LMS and TV-LMS algorithms. However, this does not apply to the RLS algorithm. Increasing the filter order in RLS algorithm does not result in any improvement in the MSE performance. Simulations also showed that the TV-LMS algorithm provides better MSE performance than the conventional LMS and the RLS algorithms with higher filter order (e.g. M=100). However, the RLS algorithm provides the best MSE performance when a small filter order is used (e.g. $M = 30$). The filter order also affects the computation time and the convergence speed of the algorithms. Increasing the filter order will rapidly increase the computation time for the RLS algorithm, whereas this does not apply to the conventional LMS and the time-varying algorithms. In terms of convergence speed, the RLS algorithm still provides a faster convergence

time. The TV-LMS algorithm can also provide a similar convergence speed with a higher filter order and a larger value for parameter C. For a single-tone signal, the TV-LMS algorithm with high filter order and larger C value will be the best algorithm as compared to the RLS algorithm and the conventional LMS algorithm in terms of computation time, convergence speed and MSE performance.

The above algorithms are also tested for noise reduction in a narrow-band QFM signal with AWGN. Results show that the proposed TV-LMS provides better MSE performance and faster convergence than the conventional LMS algorithm. The RLS algorithm under this condition gives the worst MSE performance and shows no benefit when increasing the filter order.

In the case of wideband chaos shift keying (CSK) transmitted signal, the proposed TV-LMS performs best in reducing the mean square error (MSE), while the RLS algorithm gives the worst MSE performance and slowest convergence speed. The TV-LMS has a convergence speed similar to that of the LMS algorithm.

Chapter 9

Conclusions and Future Directions

The application of chaos theory for "secure chaos communications" presents many challenging research and development problems at the basic theory, strategic, practicality, and application levels. The fundamental building blocks to construct a simple practical chaos communications, such as digital chaos generator, adaptive algorithm for chaos signal, chaos modulation schemes and demodulation techniques are already existing. However, high level frameworks for digital multimedia secure chaos communications are in need for a detailed thought. Nevertheless, further research and development are required in all fundamental building blocks to improve their robustness in practical implementation. Two major parts have been presented in this dissertation. In the first part we have discussed the development of chaos communications, studied various chaos communication and chaos signal enhancement techniques. In the second part we dealt with adaptive algorithms and their use in chaos communication. Various new approaches and applications in adaptive algorithms are looked at, e.g., the application in multiuser detection, adaptive beamforming and noise reduction for chaotic communication signals.

9.1 Summary of Results

In the first part of this dissertation, a general introduction to chaos theory is discussed in Chapter 1. In Chapter 2, a brief explanation of chaos communication theory and its history is given. An overview of various chaos communication techniques, chaotic map generators, and chaos theory applications in various areas are briefly explained. Introduction to adaptive algorithms and their application in communication engineering is presented in Chapter 2.

In Chapter 3 we provided a multimedia framework for secure chaos communication system. We proposed a modified logistic chaotic map for chaos-shift-keying (CSK) to transmit multimedia data over a highly-secure spread spectrum communication system. Both simulation and theoretical study showed that the proposed logistic chaotic map provides better performance as compared to the two existing logistic chaotic maps. In multimedia communication, we showed that user-perception is as important as the BER as a performance measure. Based on digital images, user-perception analysis showed that the additional bifurcation parameter from the proposed logistic chaotic map can potentially provide another level of security in chaos communication. This additional parameter can also be useful in the use of multiplex access (multiuser) scheme.

Chapter 4 proposed the use of diversity technique to enhance the performance of a secure chaos communication system. The proposed scheme can be used in wireless communication where security is the concern. The use of a chaotic generator for spreading can provide a more secure communication channel than using the conventional pseudo noise spreading method. Employing diversity technique is shown to provide enhancement to the chaotic signal, hence, it improves the BER performance. When a large spreading factor is

used, BER performance also improves, so is the security performance, but simulation showed that there is a threshold for this improvement after which no BER performance advantage can be obtained.

In Chapter 5, we studied the multi-carrier modulation technique for chaos communication. Three different schemes are looked at. In the first section, we proposed the use of chaos shift keying (CSK) with different orthogonal frequency division modulation (OFDM) techniques namely: CSK-OFDM and CSK- wavelet based OFDM (CSK-WOFDM). Wavelet based method (CSK-WOFDM) is shown to provide performance advantage over CSK-OFDM in terms of BER, lower PAPR value, and higher bandwidth efficiency (no guard band or cyclic prefix is needed). In the second section, we looked at the use of chaos generator to replace the conventional PN generator in CDMA communication. Simulation results showed that chaos based CDMA can provide better user detection and BER performance under multiuser environments. Chaotic sequences which are unlimited in length, aperiodic, and their bifurcation behavior provides unpredictable pattern can be useful for secure communications application. In the third section of Chapter 5, conventional OFDM-CDMA and proposed chaos based OFDM-CDMA showed to provide similar BER performance, however choas based OFDM-CDMA allows a higher number of users, a big advantage over the conventional OFDM-CDMA scheme.

The second part of the dissertation studied the adaptive algorithms for a possible application in chaos communications. Chapter 6 provided a comparative study on multiuser detection schemes for both chaos based CDMA and PN-CDMA. Two detection methods are used, the matched filtering/ correlator detection and the blind adaptive constant modulus multiuser detection algorithm. Both detection schemes showed that the chaos-based CDMA sequences

do provide enhancement in terms of BER and MSE.

In Chapter 7, we studied adaptive algorithms for beamforming application. Rather than using a fixed step-size μ (convergence parameter), we know that the antenna weight vector does contain some signal information, hence we proposed two modifications for the conventional least mean-squared (LMS) algorithm using the forward prediction of the weights vector to dynamically modify the convergence parameter. Algorithms were tested in conventional quadratic FM communication (QFM) signal as well as chaos based chaotic communication (CSK) signal. Both proposed FWV-LMS and UWV-LMS, exhibited better MMSE performance than the conventional LMS algorithm. FWV-LMS seems to be an enhanced version of LMS algorithm where performance is better but parallel to the conventional LMS behaviour. On the other hand, UWV-LMS is more adaptable to dynamic changes in the signal depending on the predicted convergence parameter, hence UWV-LMS performs better under dynamic wireless channel environment but less controlled than FWV-LMS.

Chapter 8 presented an adaptive algorithm application for noise reduction. The conventional LMS algorithm, RLS algorithm and the proposed time-varying LMS (TV-LMS) algorithm utilized a time-varying convergence parameter. Knowing that a large convergence parameter μ is needed to speed up the convergence of the filter coefficients and a smaller value of μ is needed for a more accurate estimation, the TV-LMS utilizes a decay law for the μ to provide a large value of μ at the start of the algorithm and gradually reduces μ to its optimal value. All these algorithms are tested in under additive white Gaussian noise (AWGN) with the transmitted signal as a single-tone sinusoid, non-linear quadratic FM signal, and s chaotic CSK signal. In general, TV-LMS performs better than the conventional LMS in terms of convergence speed and minimum

mean-square error. RLS algorithms are very sensitive to numerical instability, hence, it may perform better for a single-tone sinusoid but not for QFM and CSK signals.

9.2 Future Directions

Chaos can provide a promising approach for secure communications, but it is still very young. More work to be done and more practical problems to be addressed before these systems exhibit high performance in robust secure chaos communications which can put them in practical use. Based on the fundamental knowledge presented earlier, there are several areas in this dissertation that can be extended through further research as clarified below:

- In this Chapters 6, 7 and 8, we looked at the adaptive algorithm for multiuser detection application, adaptive beamforming, and noise reduction applications. Other uses of adaptive algorithms haven't been explored, and further studied of their application for different chaos communication schemes are needed.
- In this dissertation, we studied a simple adaptive LMS algorithm. Further study using other adaptive algorithms such as Kalman filter, neural networks, and other schemes can be carried out. In addition, an adaptive convergence factor within the adaptive algorithm is expected to give optimal results. This step is currently beyond the scope of this thesis.
- The combination of chaos communication with other multi-carrier modulation (MCM) schemes seems to be promising. In particular, the use of chaos communication in conjunction with wavelet multi-carrier modulation provided promising communication schemes. This can be further

studied to look at it performance in more realistic channel environments for chaos communication.

- We showed various applications of chaos in secure communications. Many of these applications are far from mature. In particular, the security issue demands further research. The study of different chaotic generator properties is needed to understand and provides a solid mathematical proof of its use to provide guaranteed quality for secure communication.
- Future multimedia data transport over a short wireless distance are likely to have a big impact on personal devices. As a result, chaos communication could provide a secure communication and is a promising candidate for this type of application. Studies of high level framework in this area should be carried out to develop a new short range secure chaos communication.
- Physical link security provided by chaos systems as shown in this thesis should be studied in conjunction with the network security provided by the transport and network layers of the general OSI communication system model.

Bibliography

[1] Y.-S. Lau, Z. M. Hussain, and R. Harris, "A Time - Varying Convergence Parameter for the LMS Algorithm in the Presence of White Gaussian Noise", *Australian Telecommunications Networks and Applications Conference 2003*, Melbourne, Australia, Dec. 2003.

[2] Y.-S. Lau, Z. M. Hussain, and R. Harris, "Performance of Adaptive Filtering Algorithms: A comparative Study", *Australian Telecommunications Networks and Applications Conference 2003*, Melbourne, Australia, Dec. 2003.

[3] Y.-S. Lau, Z. M. Hussain, and R. Harris, "A Time - Dependent LMS Algorithm for Adaptive Filtering", *WSEAS Transactions on Circuits and Systems*, Issue 1, Vol 3, Jan. 2004.

[4] Y.-S. Lau, Z. M. Hussain, and R. Harris, "A Weight-Vector LMS Algorithm for Adaptive Beamforming", in *Proc. IEEE Region 10 International Conference on Analog and Digital Techniques in Eletrical Engineering 2004*, (*TENCON'04*), Nov. 2004.

[5] Y.-S. Lau, J. Jusak, and Z. M. Hussain, "Blind Adaptive Multiuser Detection for Chaos CDMA Communication", in *Proc. IEEE Region 10*

International Conference on Analog and Digital Techniques in Eletrical Engineering 2005, (*TENCON'05*), Nov. 2005.

[6] Y.-S. Lau, T. Athanasiadis and Z. M. Hussain, "A Secure Chaos Digital Communication for Multimedia application" *Submitted to Multimedia Cyberscape Journal*.

[7] Y.-S. Lau and Z. M. Hussain, "A new approach in chaos shift keying for secure communication," in *Proc IEEE International Conference on Information Technology and Applications 2005*, Sydney, Australia, July 2005.

[8] Y.-S. Lau, and Z. M. Hussain, "Chaotic-based CDMA versus PN-based CDMA for digital secure communications: A comparative study", *Australian Telecommunications Networks and Applications Conference 2004*, Sydney, Australia, Dec. 2004.

[9] Y.-S. Lau and Z. M. Hussain, "Chaotic-based OFDM-CDMA for secure digital communications: Performance comparison with PN-based OFDM-CDMA," in *Proc The 3rd Workshop on the Internet, Telecommunications and Signal Processing (WITSP)*, Adelaide, Australia, DEC 2004.

[10] Y.-S. Lau and Z. M. Hussain, "Chaos Shift Keying Spread Spectrum with Multicarrier Modulation for Secure Digital Communication", *WSEAS Transactions on Communications*, Issue 1, Vol 4, Jan. 2005.

[11] Y.-S. Lau, K. H. Lin, and Z. M. Hussain, "Space-Time Encoded Secure Chaos Communications with Transmit Beamforming", in *Proc. IEEE Region 10 International Conference on Analog and Digital Techniques in Eletrical Engineering 2005*, (*TENCON'05*), Nov. 2005.

[12] Seedahmed S. Mahmoud, Zahir M. Hussain, and Peter O'shea, "A space-time model for mobile radio channel with hyperbolically distributed scatterers," *IEEE Antennas and Wireless Propagation Letters*, vol. 1, no. 12, pp. 211-214, 2002.

[13] A. B. cambel, *Applied Chaos Theory - A Paradigm for Complexity*, Academic Press, Inc., San Diego, CA, 1993.

[14] Gleick James, *Chaos- Making a New Science*, Penguin books, New york, NY. 1987

[15] Nicolis, and S. John, *Chaos and information processing - A heuristic Outline*, World Scientific Publishing Co. Pte. Ltd., Singapore, 1991

[16] Parker, Thomas s., Leon O.chua, *Pratical numerical algorithms for chaotic systems*, Springer-verlag new york inc, NY, 1988

[17] F. C. M. Lau, C. K. Tse, M. Ye, and S. F. Hau, "Coexistence of chaos-based and conventional digital communication systems of equal bit rate," *IEEE Trans. Circuits and Systems*, vol. 51, pp. 391-408, Feb. 2004.

[18] F. C. M. Lau and C. K. Tse, "Coexistence of chaos-based and conventional digital communication system," in *Proc IEEE ISCAS*, vol. 3, pp. III-204 - III-207, may. 2003.

[19] S. S. Rao and S. P. Howard, "Correlation performance of chaotic signals in spread spectrum systems," in *Proc IEEE Digital Signal Processing Workshop*, pp. 506-509, Sept. 1996.

[20] H.-B. Ghobad and C. D. McGillem, "A chaotic direct-sequence spread-specturm communication system," *IEEE Trans. Communications*, vol. 42, no. 234, pp. 1524- 1527, Feb/Mar/Apr. 1994.

[21] H.-B. Ghobad and C. D. McGillem, "Chaotic sequences for spread spectrum: an alternative to PN-sequences," in *Proc ICWC*, pp. 437-440, Jun. 1992.

[22] S. Kozic and T. Schimming, "Coded modulation based on higher dimensional chaotic maps," in*proc IEEE ISCAS*, vol. 2, pp. 888 - 891, 2005

[23] A. Tsuneda, D. Yoshioka, T. Hadate, "Design of spreading sequences with negative auto-correlations realizable by nonlinear feedback shift registers," in*proc IEEE Eighth International Symposium on Spread Spectrum Techniques and Applications*, pp. 330 - 334, 2004

[24] J. M. H. Elmirghani, "Data communication via chaotic encoding and associated security issues," in*proc IEEE GLOBECOM*, vol. 2, pp. 1188 - 1192, Nov. 1995

[25] T. Ushio, "Control of chaotic synchronization and secure communication systems," in*proc IEEE ETFA*, pp. 231 - 238, Nov. 1994

[26] H. Dedieu and M. J. Ogorzalek, "Identifiability and identification of chaotic systems based on adaptive synchronization," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol 44, issue 10, pp. 948 - 962, Oct. 1997

[27] Kuang-Yow Lian, Tung-Sheng Chiang, Chian-Song Chiu, and P. Liu, "Synthesis of fuzzy model-based designs to synchronization and secure

communications for chaotic systems," *IEEE Transactions on Systems, Man and Cybernetics Part B* , vol 31, issue 1, pp. 66 - 83, Feb 2001

[28] A. P. Kurian, S. Puthusserypady, and S. M. Htut, "Performance enhancement of DS/CDMA system using chaotic complex spreading sequence," *IEEE Transactions on Wireless Communications*, vol 4, issue 3, pp. 984 - 989, May 2005

[29] S. M. Htut, and S. Puthusserypady, "A novel CDP DS/SS system with 2-dimensional Ikeda map chaotic sequence," in *Proc IEEE PIMRC*, vol 3, pp. 2734 - 2738, Sept. 2003

[30] S. M. Htut, A. P. Kurian, and S. Puthusserypady, "A novel DS/SS system with complex chaotic spreading sequence," in *Proc IEEE 57th VTC 2003-Spring*, vol 3, pp. 2090 - 2094, April 2003

[31] L. Pecora and T. Carroll, "Synchronization in chaotic systems", *Phys. Rev. Lett*, vol. 64, pp. 821-824, 1990.

[32] G. Kolumban, M. P. Kennedy, and L. O. Chua, "The role of synchronization in digital communication using chaos - Part I: Fundamentals of digital communications," *IEEE Trans. Circuits and Systems I*, vol. 44, no. 10, pp. 927-936, 1997.

[33] H. Dedieu, and M. J. Ogorzaek, "Identifiability and identification of chaotic systems based on adaptive synchronization," *IEEE Trans on Circuits and Systems-I: Fundamental theory and application,*,Vol. 44, No. 10, 1997.

[34] G. Kolumban, M. P. Kennedy, and L. O. Chua, "The role of synchronization in digital communication using chaos - Part III: Performance bounds for correlator receivers," *IEEE Trans. Circuits and Systems I*, vol. 47, no. 12, pp. 1673-1683, 2000.

[35] J.M.H. Elmirghani, and R.A. Cryan, "New chaotic based communication technique with multiuser provision," *IEEE Electronics Letters,*,Vol. 30, Issue 15, pp. 1206 - 1207, 1997.

[36] J.M.H. Elmirghani, and R.A. Cryan, "Communication using chaotic masking," *IEE Colloquium on Exploiting Chaos in Signal Processing,*, pp. 12/1 - 12/6, 1994.

[37] J.M.H. Elmirghani, and R.A. Cryan, "Point-to-point and multi-user communication based on chaotic sequences," in *Proc IEEE ICC Colloquium on Exploiting Chaos in Signal Processing,*, Vol. 1, pp. 582 - 584, 1995.

[38] K. Murali, H. Leung, and H. Yu, "Design of noncoherent receiver for analog spread-spectrum communication based on chaotic masking," *IEEE Trans. Circuits and Systems I: Fundamental Theory and Applications,*, Vol. 50, Issue. 3, pp. 432 - 441, 2003.

[39] Nan Xie and H. Leung, "An analog multi-user spread spectrum technique for wireless home automation," *IEEE Trans. Consumer Electronics,*, Vol. 48, Issue. 4, pp. 1016 - 1025, 2002.

[40] H. Leung and J. Lam, "Design of Demodulator for the Chaotic Modulation Communication System," *IEEE Trans. Circuits and Systems I: Fundamental Theory and Applications,*, Vol. 44, No. 3, pp. 262 - 267, 1997.

[41] Tommy W. S. Chow, Jiu-Chao Feng, and K.T. Ng, "An Adaptive Demodulator for the Chaotic Modulation Communication System with RBF Neural Network ," *IEEE Trans. Circuits and Systems I: Fundamental Theory and Applications,*, Vol. 47, No. 6, pp. 902 - 909, 2000.

[42] C. L. Koh and T. Ushio, "Digital Communication Method Based on - Synchronized Chaotic Systems," *IEEE Trans. Circuits and Systems I: Fundamental Theory and Applications,*, Vol. 44, No. 5, 1997.

[43] G. Kolumban, "Theoretical Noise Performance of Correlator-Based Chaotic Communications Schemes," *IEEE Trans. Circuits and Systems I: Fundamental Theory and Applications,*, Vol. 47, No. 12, 2000.

[44] G. Mazzini, G. Setti, and R. Rovatti "Chaotic Complex Spreading Sequences for Asynchronous DS-CDMAŮPart I: System Modeling and Results," *IEEE Trans. Circuits and Systems I: Fundamental Theory and Applications,*, Vol. 44, No. 10, 1997.

[45] Riccardo Rovatti, Gianluca Mazzini, and Gianluca Setti "Enhanced Rake Receivers for Chaos-Based DS-CDMA," *IEEE Trans. Circuits and Systems I: Fundamental Theory and Applications,*, Vol. 48, No. 7, 2001.

[46] Gianluca Mazzini, Riccardo Rovatti, and Gianluca Setti "Chaos-Based Asynchronous DS-CDMA Systems and Enhanced Rake Receivers: Measuring the Improvements," *IEEE Trans. Circuits and Systems I: Fundamental Theory and Applications,*, Vol. 48, No. 12, 2001.

[47] Riccardo Rovatti, Gianluca Mazzini, and Gianluca Setti "On the Ultimate Limits of Chaos-Based Asynchronous DS-CDMAŮI: Basic Definitions and Results," *IEEE Trans. Circuits and Systems I,*, Vol. 51, No. 7, 2004.

[48] J. Schweizer and T. Schimming "Symbolic Dynamics for Processing Chaotic SignalsŮII: Communication and Coding," *IEEE Trans. Circuits and Systems I,*, Vol. 48, No. 11, 2001.

[49] K. M. Cuomo, A. V. Oppenheim, and R. J. Barron, "Synchronization of Lorenz-based chaotic circuits with applications to communications," *IEEE Trans. Circuits and Systems II,*, Vol. 40, pp. 626-633, 1993.

[50] K. M. Cuomo and A. V. Oppenheim, "Circuit implementation of synchronized chaos with applications to communications," *Physic Rev. Lett,*, Vol. 71, pp. 65-68, 1993.

[51] G. Kolumban, M. P. Kennedy, Z. Jako, and G. Kis, "Chaotic communications with correlator receivers: theory and performance limits," in *Proc of the IEEE*, vol. 90, pp. 711-732, 2002.

[52] A. Abel and W. Schwarz, "Chaos CommunicationsŮPrinciples, Schemes, and System Analysis," Invited paper in *IEEE Proc,* Vol. 90, No. 5, May 2002.

[53] C. K. Tse, K. Y. Cheong, F. C. M. Lau and S. F. Hau, "An approach for CSK detection based on return maps," in *Proc of Int. Symp. on Nonlinear Theory and Its Appl,* pp. 637 - 640, 2001.

[54] A. Dmitriev, B. Kyarginsky, A. Panas, and S. Starkov, "Direct chaotic communication system. Experiments," in *Int. Workshop Nonlinear Dynamics in Electronic Systems,* pp. 157 - 160, 2001.

[55] G. Kolumban, B. Vizvari, W. Schwarz and A. Abel, "Differential chaos shift keying: A robust coding for chaotic communication," in *Proc. of the*

Fourth Int. Workshop on Nonlinear Dynamics of Eletronic Systems, pp. 87-92, 1996.

[56] J. M. Ottino, F. J. Muzzio, M. Tjahjadi, J. G. Franjioe, S. C. Jana and H. A. Kusch, "Chaos, symmetry and self-similarity: Exploiting order and disorder in mixing process," *Science*, vol. 257, pp. 754-760, 1992.

[57] R. S. Mackay, "Some Thoughts on chaos in engineering, in toward the harnessing of chaos," *Elservier Science*, pp. 73-82, 1994.

[58] V. I. Vorotnikov, "Optimization of vibration drilling process," *Transcations of Bauman Moscow State Techncal Univ*, no. 332, 1980.

[59] H. D. Chiang, C. W. Liu, P. P. Varaiya, F. F. Wu and M. G. Lauby, "Chaos in a simple power system," *IEEE Trans. Power System*, vol. 8, no. 4, pp. 1407-141, 1993.

[60] B. Lee, and V. Ajjarapu, "Period-doubling route to chaos in an electrical power system," *IEE Proceedings-Generation, Transmission and Distribution*, vol. 140, issue. 6, pp. 490-496, 1993.

[61] H. O. Wang, E. H. Abed and A. and M. A Hamdan, "Bifurcation, chaos and crises in voltage collapse of a model of power system," *IEEE Trans. Circuits and Systems I*, vol.41, no. 3, pp. 294-302, 1994.

[62] L. A. Dissado, "Deterministic chaos in breakdown. Does it occur and what can it tell us?," *IEEE Trans. Dielectrics and Electrical Insulation*, vol. 9, issue. 5, pp. 752-762, 2002.

[63] Ljupco Kocarev, "Chaos-Based Cryptography: A Brief Overview," *IEEE Communication Magazine,* Vol 1, Issue 3, pp. 6 - 21, 2001.

[64] P. Bergamo, P. DŠArco, A. D. Santis, and L. Kocarev, "Security of Public-Key Cryptosystems Based on Chebyshev Polynomials," *IEEE Trans. on circuits and system I,* Vol 52, No. 7, 2005.

[65] T. Yang, C. W. Wu, and L. O. Chua, "Cryptography Based on Chaotic Systems," *IEEE Trans. on circuits and system I,* Vol 44, No. 5, 1997.

[66] B. Chen and G. W. Wornell, "Analog Error-Correcting Codes Based on Chaotic Dynamical Systems," *IEEE Tran on Communications,* Vol 46, No. 7, 1998.

[67] S. Tang, H. F. Chen, S. K. Hwang and J. M. Liu, "Message encoding and decoding through chaos modulation in chaotic optical communications," *IEEE Trans. on circuits and system I,* Vol 49, No. 2, pp. 163 - 169, 2002.

[68] S. Tang and J. M. Liu, "2.5 Gb/s chaotic optical communication," in *IEEE Proc. OFC,* pp. 402 - 404, 2002.

[69] J. M. Liu, H. F. Chen and S. Tang and , "Synchronized chaotic optical communications at high bit rates," *IEEE Trans. Quantum Electronics,* Vol 38, Issue. 9, pp. 1184 - 1196, 2002.

[70] D. Kanakidis, A. Argyris, and D. Syvridis, "Performance characterization of high-bit-rate optical chaotic communication systems in a back-to-back configuration," *IEEE Trans. Lightwave Technology,* Vol 21, Issue. 3, pp. 750 - 758, 2003.

[71] S. Haykin, *Adaptive Filter Theory,* Prentice Hall, 1986.

[72] B. widrow, S. D. Stearns, *Adaptive Signal Processing*, Prentice Hall, 1985.

[73] Zhiwen Zhu and Henry Leung, "Adaptive Identification of Nonlinear Systems with Application to Chaotic Communications," *IEEE Trans. on circuits and system,* Vol 47, No. 7, 2000.

[74] P. S. Kah and K. M. Tse, "Investigation of several demodulation schemes using adaptive filter in chaotic communication systems," in *IEEE Proc. APCC 2003,* Vol 2, pp. 834 - 837, 2003.

[75] A. Muller and Jaafar M. H. Elmirghani, "Blind Channel Estimation and Echo Cancellation Using Chaotic Coded Signals," *IEEE Lett. on Communications,* Vol 3, No 3, pp. 72 - 74, 1999.

[76] B.-Y. Wong and W. X. Zheng, "Blind adaptive channel identification/equalication in chaotic communications by using nonlinear prediction technique," in *IEEE Proc. ICSP'04,* 2004.

[77] M. P. Kennedy and G. Kolumban, "Digital communications using choas," *Elsevier Signal Processing Journal*, vol. 80, pp. 1307-1320, 2000.

[78] T. Kohda and A. Tsuneda, "Even- and odd-correlation fucntions of chaotic chebyshev bit sequences for CDMA," in *Proc. IEEE Int. Symp. Spread Specturm Technology and Applications*, pp. 391-395, 1994.

[79] M. Ibnkahla, *Signal Processing for Mobile Communications Handbook*, CRC Press, ch. 10, 2005.

[80] J.F. Huber, "Mobile next-generation networks", *IEEE Multimedia*, vol. 11, pp. 72-83, Jan-Feb 2004.

[81] T. S. Rappaport, *Wireless Communications Principles and Pratice*, 2nd ed, Delhi, India: Person Education Inc, 2002.

[82] M. Ghanbari, "Standard CodesL Image Compression To Advanced Video Coding", Herts, Uk: The institution of Electrical Engineerd, *IEE Telecommunications*, Series 49, 2003.

[83] S. Catreux, V. Erceg, D. Gesbert and R.W. jr. Heath, "Adaptive modulation and MIMO coding for broadband wireless data networks", *IEEE Communication Magazine*, vol. 40, pp. 108-115, Jun 2002.

[84] M. Kr. Mandal, *Multimedia Signals and Systems*, Massachusetts. USA: Kluwer Academic, 2003.

[85] Website of ECE, Rice University: http://www.dsp.ece.rice.edu/wakin/images/lena512.bmp , last visited Dec 2004.

[86] K. H. Lin, Z. M. Hussain, and R. J. Harris, "Space-time OFDM with adaptive beamforming: Performance in spatially correlated channels," in *Proc. IEEE TENCON*, ChiangMai, Nov. 2004, pp. 617-620.

[87] G. Ganesan, P. Stoica, and E. G. Larsson, "Diagonally weighted orthogonal space-time block codes," *Thirty-Sixth Asilomar Conference on Signals, Systems and Computers*, vol. 2, Nov. 2002, pp. 1147-1151.

[88] V. Tarokh, H. Jafarkhani, and A. R. Calderbank, "Space-time block codes from orthogonal designs," *IEEE Trans. Inform. Theory*, vol. 45, pp. 1456-1467, July 1998.

[89] V. Tarokh, H. Jafarkhani, and A. R. Calderbank, "Space-time block coding for wireless communications:Performance results," *IEEE J. Select. Areas in Commun.*, vol. 17, pp. 451-460, Mar. 1999.

[90] E. G. Larsson and P. Stoica, *Space-Time Block Coding for Wireless Communications*. Cambridge, U.K.: Cambridge Univ. Press, 2003.

[91] Siemens, *Channel Model for Tx Diversity Simulations using Correlated Antennas*, 3GPP Document TSG-RAN WG1 #15, R1-00-1067, Berlin, Germany, Aug. 2000.

[92] J. G. Proakis, *Digital Communications*, New York, N.Y.: McGraw-Hill Inc., Fourth Edition, 2001.

[93] S. B. Weinstein, and P. M. Ebert "Data transmission by frequency-division multiplexing using the discrete fourier transform," *IEEE Trans. Communication Technology*, vol. 19, No. 5, pp. 628-634, Oct 1971.

[94] Rainmaker Technologies, Inc., "RM wavelet based PHY proposal for 802.16.3," http://ieee802.org/16.

[95] G. W. Wornell, and A. V. Oppenheim "Wavelet-based representations for a class of self-similar signals with application to fractal modulation," *IEEE Trans. Information Theory*, Vol. 38, No. 2 pt II, Special iss, pp. 785-800, 1992.

[96] G. W. Wornell, and A. V. Oppenheim "Estimation of fractal signals from noisy measurements using wavelet," *IEEE Trans. Signal Processing*, Vol. 4, No. 3, pp. 611-623, May 1992.

[97] F. Zhao, H. Zhang, and D. Yuan, "Performance of COFDM with different orthogonal bases on AWGN and frequency selective channel," in Proc. *IEEE 6th CAS Symp. on Emerging Technologies: Mobile and Wireless Comm.*, pp. 473-475, May 2004.

[98] J.-A. Tsai, C.-L. Hsiao, S.-K. Lee and C.-L. I, "Performance analysis of adaptive beamforming for OFDM-CDMA systems in ground-based communications," in *IEEE Proc. The Thrity-seventh Asilomar Conference on Signals, System & Computers*, pp. 643-646, Nov. 2003.

[99] S. Hara and R. Prasad, "Overview of multicarrier CDMA," *IEEE Communications Magazine*, vol. 35, pp. 126-133, Dec. 1994.

[100] S. Kaiser, "OFDM code-division multiplexing in fading channels," *IEEE Trans. Communications*, vol. 50, pp. 1266-1273, Aug. 2002.

[101] M. Abolbashari, and H. Aghaeinia "Design and analysis of a new sequence set by using chaotic dynamic systems for spread specturm communication applications," in *Proc ICCT*, pp. 917-921, Apr. 2003.

[102] T. K. Sarkar, M. Salazar-Palma, and M. C. Wicks, *Wavelet Applications in Engineering Electromagnetics,* Artech House Publishers, 2002.

[103] R. Rovatti, G. Mazzini, and G. Setti, "On the ultimate limits of chaos-based asynchronous DS-CDMA I : Basic Definitions and Results " *IEEE Trans. Circuit and Systems*, vol. 51, pp. 1336-1347, July 2004.

[104] R. Rovatti and G. Mazzini "Interference in DS-CDMA systems with exponentially vanishing autocorrelations: Chaos-based spreading is optimal," *Electron. Lett.*, vol. 34, 1998.

[105] G. Mazzini, R. Rovatti, and G. Setti, "Interference minimization by autocorrelation shaping in asynchronous DS-CDMA systems: Chaos-based spreading is nearly optimal," *Electron. Lett.*, vol. 35, 1999.

[106] T. kohda and H. Fujisaki, "Variances of multiple access interference code average agianst data average," *Electron. Lett*, vol. 36, 2000.

[107] S. Moshavi, "Blind Adaptive Multiuser Detection," *IEEE Tran. on Information Theory*, vol. 41, no. 4, pp. 944-960, July 1995.

[108] M. Honig and M. K. Tsatsanis, "Adaptive Techniques for Multi-user CDMA Receivers," *IEEE Signal Processing Magazine*, vol. 34, pp. 49-61, May 2000.

[109] J. Jusak and Z. M. Hussain, "Low Complexity Blind Adaptive Multi-User Detection for Up-link DS-CDMA," *Australian Telecommunications, Networks and Applications Conference (ATNAC)*, Sydney, Australia, 2004.

[110] C. R. Johnson, Jr., P. Schnitter, T. J. Endres, et al., "Blind Equalization Using the Constant Modulus Criterion: A Review," *IEEE Proceedings*, vol. 86, No. 10, pp. 1927-1950, October 1998.

[111] John Litva and Titus Kwok-Yeung Lo, *Digital Beamforming in Wireless Communications*, Artech House Publishers, 1996.

[112] A. J. Paulraj, D. Gesbert, and C. Papadias, "Smart antennas for mobile communications" *Encyclopedia For Electrical Engineering*, John-Wiley Publishing Co., 2000.

[113] L. Cohen, *Time-Frequency Anaysis,* Prentice-Hall, 1995.

[114] M. H. Hayes, *Statistical Digital Signal Processing and Modeling,* John Wiley & Sons, 1996.

[115] S. Nahm, and W. Sung, "Time-domain equalization for orthogonal multi-carrier CDMA system," *Global Telecommunications Conference*, vol. 30, 1996.

[116] D. N. Kalofonos, M. Stojanovic, and J. G. Proakis, "On the performance of adaptive MMSE detectors for MC-CDMA system in fast fading Rayleigh channels," *The Ninth IEEE International Symposium on Personal, Indoor and Mobile Radio Communications,*, vol. 3, 1998.

VITA

Yuu-Seng Lau received his double degree Bachelor of Engineering (Electronics) and Bachelor of Applied Science (Computer Science) from RMIT University, Melbourne, Australia in 2001. He worked as a Research Engineer and a Technical Consultant in various companies. He has currently finished his PhD (Digital Communications) at the School of Electrical and Computer Engineering, RMIT University, Melbourne, Australia. His research interests are mobile communications, applied signal processing, communications infrastructure, secure communications, games, artificial intelligence, and adaptive learning algorithms.